Cybercriminology TLS_0037, TY Spring 2009 Course Snapshot

Xingan Li, LLD
Faculty of Law
University of Turku

What is Cybercriminology?

- Cyber, =computer, computer network
  - (cyber-A prefix that means "computer" or "computer network," as in *cyberspace,* the electronic medium in which online communication takes place. See The American Heritage® Science Dictionary Copyright © 2005 by Houghton Mifflin Company.)
- Cybercrime, =computer crime, or network crime
- Cybercriminology, =science of computer crime

How is cybercriminology like?

- It is like criminology. How? All of crime, all about crime, and all against crime: phenomena, causes, countermeasures, and policy.
- It is about cybercrime. How? All of cybercrime, all about cybercrime, and all against cybercrime.
- It is new. Cybercrime is 50 years old or so? What subject is as new as cybercriminology?
- It is developing fast. Number of criminals, number of offences, number of potential victims, and forms of offences are changing fast.

Cybercriminology: a subdiscipline of criminology?

- Criminology is a subject with broad research scope. Almosrt everything about crime can be studied there.
- Cybercrime can be studied within the framework of criminology.
- However, in order to accumulate knowledge and understanding, cybercrime can also be studied first independently as a subdiscipline, then integrated into criminology.
- It is not an ultimate goal to create a subdiscipline, but a means to study cybercrime.

Synopsis

- AIM AND CONTENT:
- The course aims at introducing students to fundamental aspects of cybercriminology, with both practical and methodological issues tackled. Phenomena, countermeasures and research methods constitute a triplet of this course.
- The course will primarily cover the following topics:
- Contextual introduction to cybercrime
- Proposed ways to recognize cybercrime
- A complex of countermeasures
- A bundle of alternative methods for research in cybercriminology
- Legal, ethical, political and other dilemmas

- FORMAT: Lectures, and discussions, 15 hours. Essay, independent work.
- LEVEL: Intermediate/Advanced

Lecture Schedule

- 23 Jan. 10-11
- 30 Jan., 10-12
- 6 Feb., 10-12
- 13 Feb., 10-12
- 20 Feb., 10-12
- 27 Feb., 10-12
- 6 March, 10-12
- 13 March, 10-12
- Course homepage: http://users.utu.fi/xinli/cc.html

- Venue: Cal. 2

Recommended Readings (1)

- CSI/FBI. 2008. Computer Crime and Security Survey, 2008. Available at http://www.gocsi.com/forms/csi_survey.jhtml
- Goodman, Marc D. and Brenner, Susan W. 2002. The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol.6, Issue 1. Available at http://www.lawtechjournal.com/articles/2002/05_021229_roemer.pdf
- Katyal, Neal Kumar. 2003. Digital Architecture as Crime Control, The Yale Law Journal, Vol. 112, No. 8, pp. 2261-2289. Available at http://yalelawjournal.org/images/pdfs/142.pdf
- Li, Xingan. 2008. Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society, Turku: Uniprint.
- Rogers, Marcus K. 2001. A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Explanatory Study, Winnipeg, Manitoba: University of Manitoba. Available at http://homes.cerias.purdue.edu/~mkr/cybercrime-thesis.pdf

Recommended Readings (2)

- Rustad, Michael L. 2001. Private Enforcement of Cybercrime on the Electronic Frontier, Southern California Interdisciplinary Law Journal, Vol. 11, pp. 63-116.
- Skinner, William F. and Fream, Anne M. 1997. A Social Learning Theory Analysis of Computer Crime among College Students, Journal of Research in Crime and Delinquency, Vol. 34, No. 4, pp. 495-518. Available at http://jrc.sagepub.com/cgi/reprint/34/4/495
- Yar, Majid. 2005. The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory, European Journal of Criminology, Vol. 2, No. 4, pp. 407-427. Available at http://euc.sagepub.com/cgi/reprint/2/4/407

Evaluation

- Evaluation based on
- 1. Active participation in lectures.
- 2. A 5-minute prepared talk about your understanding of cybercrime on 13 March.
- 3. An essay of 10-15 A4 pages, MS Word format, font Times New Roman, size 12 pt, and line spacing 1.5.

- Topic deadline: 13 March, 2009 (sent to email: xingan.li@yahoo.com)
- Essay deadline: 13 April, 2009 (sent to email: xingan.li@yahoo.com)
- Grading: 1-5

Cybercriminology
Definition and Classification of Cybercrime

Xingan Li, LLD
Faculty of Law
University of Turku

DOI: 10.13140/2.1.4586.3209

Definition and Classification of Cybercrime

- Earlier notions of computer crime
- The previous deficiencies in understanding cybercrime
- What exactly is cybercrime?
- “Cyber” as a label of crime
- Towards a broad definition of cybercrime
- Proposed definition of cybercrime

Earlier notions of computer crime

- From the first standpoint, there was no such thing as computer crime.
- For example, Johnson (1985) insisted that there was no distinction between an offence involving a computer and an offence involving no computer. Gotternbarn (1990, pp. 18-24) also claimed that a particular category of computer crime was unnecessary. The negativists regarded computer crimes as offences belonging to traditional categories.

- The second standpoint claimed that the computer could be used to perpetrate every kind of crime. It could be considered pan-computer crime view (Nycum 1983, pp. 2-4).
- According to Sterling (1994), Donn B. Parker claimed that "…all business crime will be computer crime, because businesses will do everything through computers. 'Computer crime' as a category will vanish."

- The third standpoint was held by middle-of-the-roaders, admitting the existence of computer crime, but limited the range of offences on the other.
- Different technical terms have been used to denote the phenomenon, different definitions have been given to describe the issue, and different theoretical achievements have been acquired to address the legal framework. However, there has never been a unified technical term, a unified definition (UNCJIN 1999, Paragraph 21), or a unified theoretical structure.

- Computer crime has been defined in a diverse spectrum of senses, from extremely narrow ones to extremely broad ones. The definition in the narrowest sense limits computer crime to “one that can be carried out only through the use of computer technology” (Tavani 2000, pp. 6-7). This definition excludes crimes that can be committed only through other means than computer technology and that can be committed in both ways.

- A broader approach defines computer crime as crime by computer. This definition excludes crimes targeting a computer.

- A yet broader definition includes both crimes by computer and against the computer.
- The development of cybercriminal phenomena proves that there is a vague limit between offences by computer and offences against the computer.

- The broadest definition was proposed by Parker (1980, cited in Solarz 1981, pp. 25-26), who divided computer crimes into computer abuse, computer crime and computer-related crime.

The previous deficiencies in understanding cybercrime

- Some of the previous understanding about cybercrime has been misleading and confusing in providing inexact information.
- The first misunderstanding happened against a historical background:
  - Hacking is cybercrime

- The increasing cyber perpetration at the end of the 20th century and the beginning of the 21st century witnessed a second misunderstanding of the conception. The illusion that information systems were a critical infrastructure that was easily prone to abuse and in effect caused massive deaths, injuries, and economic disasters led to an extreme notion that viewed all cybercrimes as terrorist attacks.
    - Cybercrime is cyberterrorism

- The third misunderstanding is politicization of the conception in a broader sense:
  - Information systems are National Information Infrastructure
  - Cybercrime (act against information system) is crime against state security (act against NII)

- The fourth misleading understanding is, strangely, to moralize the cybercrime by exploiting the term “hacking”.
    - Cybercrime is hacking, while
        - Hacking is ethical

- The last category of misleading definitions has the tendency of mystification.
    - Cybercrime is high-tech crime…

What exactly is cybercrime?

- No unified term for cybercriminal phenomena has been universally accepted, even though some terms including “computer crime” and “cybercrime” are relatively popular.

- The first group of terms emphasizes the view that regards the computer as a unique target or tool of crime. The term “computer crime” has been broadly used in academic writings as well as in laws and regulations particularly before the Internet was opened to commercial use in the 1990s.
- This term represents a group of similar terms, including computer crime, crime by computer (Parker 1976), computer-related crime (Sieber 1998; Stephenson 2000), computer-facilitated crime, computer misuse, computer abuse, computer mischief, computer break-in, computer sabotage (Sieber 1996), computer espionage, computer manipulation (Sieber 1996), etc. “Comcrime” was used in the title of Sieber (1998), though the term was not used in the main body of the text.

- The second group of terms are accompanied with a crime particularly facilitated by computer networks. The origin of the term “cybercrime” cannot be identified, but there is no doubt that it became prevalent with the legislating process of the European Convention on Cybercrime.
- Most authors are using these two terms interchangeably. Besides terms cybercrime, or cyber crime, people also use net crime, the Internet crime (Taylor and Quayle 2003), crime on the Internet, Internet-related crime, network crime, etc.

- The third group of terms regard the Internet as only a part of the whole telecommunications systems. Electronic crime (e-crime) emphasizes the characteristic of the criminal phenomena relating to (micro) electronics rather than to computer or computer networks.

- The fourth group of terms regard the space, the community, or the environment created by the Internet as the place where a crime is committed. The word “virtual” has a deep and different meaning in the term “virtual reality”,but “virtual crime” is in fact the substitute of cybercrime in the sense that the crime is committed in the network environment.

- The fifth group of terms regard the data, information or privacy as the primary factor in a crime. In fact, cybercrime is crime related to information or information systems (not limited to computer and computer networks).

- The sixth group of terms regard the processing of “digital” information as the unique characteristic of cybercrime (Lilley 2002).

- The seventh group of the terms regard ICT as high technology.
- A crime involving ICT is named high technology crime, high-tech crime, hi-tech crime, or information technique crime.

"Cyber" as a label of crime

- The label contains the implicit meaning of deviant behaviours dependent on information systems.
- The label sketches the semi-virtual and semi-real crime scene.
- The label gives us an impression of human-machine criminal interactions.
- The label demonstrates on extension of the criminal territory.
- (to be continued)

- The label causes multidisciplinary attention. In the past, scholars attempted to label all those disciplines relating to crime by the term “criminal” and formed many marginal disciplines, such as criminal psychology, criminal sociology, etc.
- The label holds the digital criminal power.
- The label does not disrupt the vitality and continuity of the criminal tradition.
- The label confirms the transformation of criminal patterns.

Towards a broad definition of cybercrime

- First, help to achieve as great a consensus as possible in the context of criminal-law reform.
- Secondly, help to revise criminal law completely, thus avoiding merely adding simply a couple of isolated provisions.
- Thirdly, help to amend procedural criminal law based on substantive criminal law.
- Finally, also help to provide full protection for a critical information infrastructure.

Proposed definition of cybercrime

- Cybercrime is defined as any type or any form of traditional or untraditional crime involving information systems in use as media, means, place, route, target, tool, or used in the preparation for other crimes.

- First, cybercrime covers any form of traditional or any type of untraditional crime that can involve information systems.
- Second, information systems are the distinct factor in cybercrime.
- Thirdly, information systems must be in use.
- Fourthly, the roles of information systems in cybercrime are multiple.
- Finally, it is also necessary to point out that, even if we adopt a broad definition of cybercrime, the offences merely involving information systems but having nothing to do with their functions do not constitute cybercrime.

Categories of cybercrime

- Information systems as a target of the offence
- Information systems as a tool of the offence
- Information systems as a medium for the offence
- Information systems as a route to the offence
- Information systems as a place of the offence
- Information systems as means of the offence
- Information systems used in preparation for other offences

Information systems as a target of the offence

- 1. Unauthorized access to information systems,
- 2. Unauthorized access to information,
- 3. Unauthorized alteration of information,
- 4. Unauthorized interruption of information systems,
- 5. Attack by viruses, worms, logic bomb, Trojan horse, and other malicious programmes,
- 6. Theft of computer time, network time, or telecommunications services, a specific form of illegal access,
- 7. Possession, disclosure and providing unauthorized persons with unauthorized information; or unauthorized possession, disclosure and providing unauthorized persons with information, both being the extension of illegal access to information.
- 8. Unauthorized interception of communications.

Information systems as a tool of the offence

- 1. Forgery and counterfeiting,
- 2. Computer-aided unauthorized copy of software and other copyrighted works,
- 3. Telecommunication piracy,
- 4. Fraud using information systems,
- 5. Password sniffering and keylogging.

Information systems as a medium for the offence

- 1. Dissemination of obscene material, in particular child pornography,
- 2. Dissemination of racist and xenophobic material through computer systems,
- 3. Online false statement about individuals or corporations,
- 4. Indecent exposure,
- 5. False advertising,
- 6. Disclosure of confidential information.

Information systems as a route to the offence

- 1. E-mail bombing,
- 2. Harassment through electronic communication,
- 3. Identity theft and cyberstalking,
- 4. Denial of service attacks (cyber terrorism),
- 5. Distribution of pirated software, books, magazines, audio, video or live performances, etc.,
- 6. Infringement of industrial secrets and state secrets,
- 7. Transmission of child pornography.

Information systems as a place of the offence

- 1. Intellectual property infringement,
- 2. Collection and exhibition of child pornography,
- 3. Sale of illegal articles (such as fire arms, alcohol, prescriptive drugs and other controlled substances),
- 4. Online (illegal) gambling,
- 5. Fraud on the Internet (such as Internet auction fraud, multi-level marketing fraud).

Information systems as means of the offence

- 1. Electronic extortion, harassment, creating a false alarm, threatening, and assault,
- 2. E-mail spoofing (phishing).

Information systems used in preparation for other offences

- 1. Communications in furtherance of criminal activity or criminal conspiracy,
- 2. Electronic money laundering,
- 3. Online tax evasion,
- 4. E-mail spoofing (phishing).
- 5. Child exploitation.

Clarification of relevant conceptions

- White-collar crime
- Economic crime
- Corporate crime
- Professional crime
- Trans-national crime

White-collar crime

- The conception of white-collar crime was coined by Edwin H. Sutherland in 1939 and defined “approximately as a crime committed by a person of respectability and high social status in the course of his occupation” (Sutherland 1949, p. 9).

Economic crime

- Sjögren and Skogh (2004, p. 1) defined economic crime as a crime committed to gain profit within an otherwise legal business. Recommendation No. R (81) 12 of the Council of Europe's Committee of Ministers of 1981 listed a broad range of offences into economic crime, including computer crime, particularly theft of data, violation of secrets, and manipulation of computerized data. The relevant literature has taken it as natural that computer crime is a crime in which the computer is used as an instrument of economic crime (for example, Johnson 2006, p. 1).

Corporate crime

- Yeager and Clinard (2006) have defined corporate crime as “any act committed by corporations, that is punished by the state, regardless of whether it is punished under administrative, civil, or criminal law” (p. 16) and they have regarded it as a particular type of white-collar crime (p. 17). It is possible for corporations to commit cybercrime, and the relationships between these conceptions are become ever more puzzling.

Professional crime

- Overall, insiders and outsiders constitute 21 percent and 79 percent of all reported offenders separately classified. Former employees constitute 16 percent of all the outsiders. If we add up former employees into insiders, they would constitute about 34 percent of the total number of offenders, still a smaller ratio than the outsiders. Cybercrime is not a professional or occupational crime.

Trans-national crime

- First, information systems have crossed the national boundaries, but prosecuted offences are mostly confined within these boundaries;
- Second, due to lack of an international arrangement of law and enforcement, few trans-national cybercrime offenders have been investigated; and
- Third, offences are mostly territory-dependent, and do not cross the border at all.

Conclusion

- The phenomenon of cybercrime is developing, thus recognition of it should also be developed.
- It is easy to define it in a narrow sense, but it should be careful when define it in a broad sense .
- Definition and classification are metaphorical.

Primary types of cybercrime, anyway? Just name some:

Counterfeiting Creating, spreading, disseminating, and sending computer viruses, worms, Trojan horses, spyware Cyber pornography Cyberstalking Dafamation Defacement (webjacking) Dissemination of obscene material DoS attack Email bombing Email spoofing Espionage against enterprises and states Infringement of privacy Forgery	Fraud Hacking and cracking Harassment Identity theft Intellectual Property crimes Internet time thefts Logic bombs Online gambling Phishing and pharming Sale of illegal articles Spamming Trafficking in drugs, human beings, arms weapons Vandalism ……

References

- Gotterbarn, D. 1990. Computer Ethics: Responsibility Regained, National Forum: The Phi Kappa Phi Journal, volume 71, number 3, pp. 26-31.
- Johnson, D. G. 1985. Computer Ethics, Englewood Cliffs, New Jersey: Prentice Hall.
- Li, X. 2008. Cybercrime and Deterrence, Uniprint.
- Lilley, P. 2002. Hacked, Attacked, and Abused: Digital Crime Exposed, London, U. K.: Kogan Page Limited.
- Nycum, S. H. 1983. Testimony on Computer Security before the U. S. Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computers and Society, volume 13, number 4 and volume 14, Nos. 1, 2, and 3.
- Parker, D. B. 1976. Crime by Computer, New York: Charles Scribner's Sons.
- Sieber, U. 1996. Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society - Statement for the Hearing on Security in Cyberspace of the United States Senate, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, 16 July.
- Sieber, U. 1998. Legal Aspects of Computer-Related Crime in the Information Society, The COMCRIME-Study for the European Commission. Retrieved 15 March 2007, from http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html

- Sjögren, H., and Skogh, G. 2004. Introduction, In H. Sjögren and G. Skogh eds. New Perspectives on Economic Crime, Edward Elgar Publishing, pp. 1-4.
- Solarz, A. 1981. Computer Technology and Computer Crime, Stockholm, Sweden: Research and Development Division.
- Stephenson, P. 2000. Investigating Computer-Related Crime, Boca Raton: Florida: CRC Press LLC.
- Sterling, B. 1994. The Hacker Crackdown: Law and Disorder on the Electronic Frontier, Austin, Texas: Electronic Release. Retrieved 15 March 2007, from http://www.gutenberg.org/dirs/etext94/hack12.txt
- Sutherland, E. H. 1949. White Collar Crime, New York: Holt, Rinehart and Winston.
- Tavani, H. T. 2000. Defining the Boundaries of Computer Crime: Piracy, Break-ins, and Sabotage in Cyberspace, Computers and Society, volume 30, number 4, pp. 3-9.
- Taylor, M. and Quayle, E. 2003. Child Pornography: An Internet Crime, East Sussex: Brunner-Routledge.
- UNCJIN. 1999. International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime, International Review of Criminal Policy, nos. 43 and 44.
- Yeager, P. and Clinard, M. 2006. Corporate Crime, Transaction Publishers.

- Any questions?

Cybercriminology
Cyberspace and Cybercrime

Xingan Li, LLD
Faculty of Law
University of Turku

DOI: 10.13140/2.1.1014.6087

The Internet in Human History

- Calculated by 1-million-year span, what were the most famous historical event do you remember? Archaeologists found some fossils and said that they belonged to our earliest ancestors.
- By 100,000-year span? Our ancestors could have learned to use fire. 10,000-year span? Our ancestors could have learned to plant crops and feed animals. 1-millenium span? Suddenly, there were too many things we have to remember, of them were birth of some religions, existence of some civilizations. 1-century span? Wars and revolutions. 1-decade span? Bush, Blair and Putin?
- In recent decade, one of the most significant thing is that all of us are connected online.

Once connected, never disconnected.

- Writers usually let us imagine a world or a society without fire and light, without civilization, without electricity, without cars and roads, and without the Internet.
- Social phenomena can never be reversed, including crime.

A process of cyberization

- Some indicators for describing the process of cyberization:

1. the number of personal computers (PCs) and the Internet users
2. the increase in the number of web sites
3. the number of Internet hosts
4. the number of web pages
5. bandwidth growth
6. the growth of scale of e-commerce

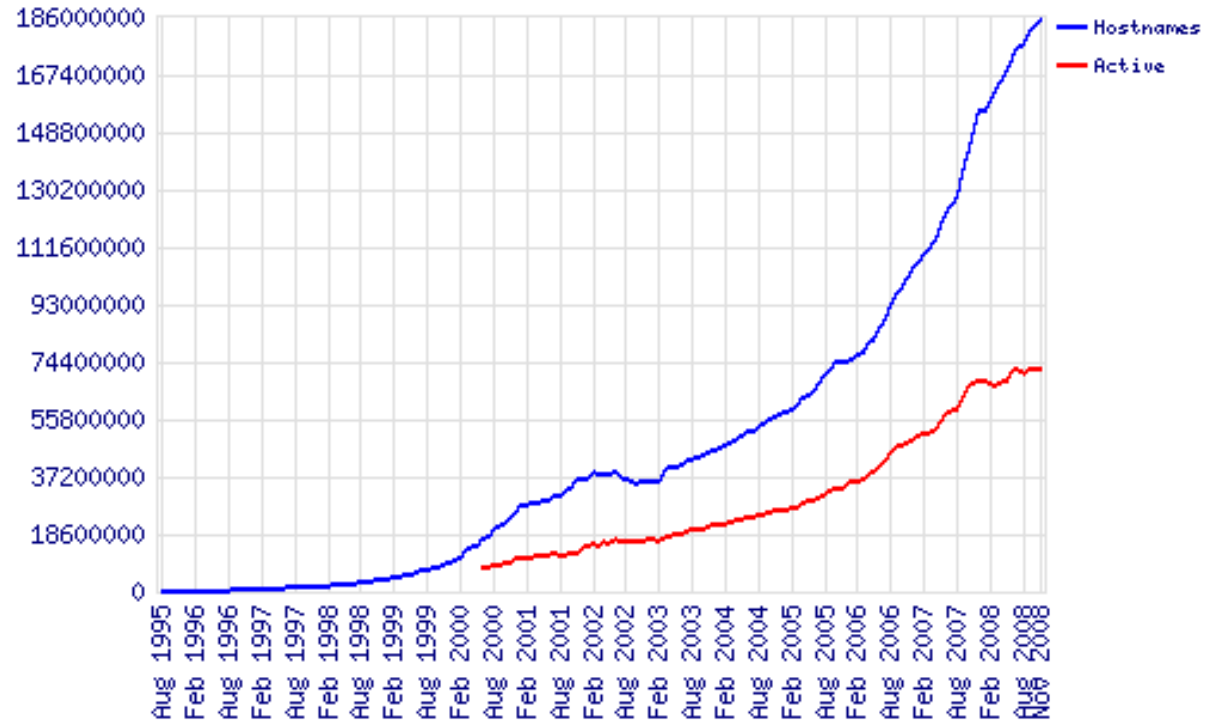
Number of personal computers (PCs) and Internet users

- The first indicator is the number of personal computers (PCs) and the Internet users.
- According to the International Telecommunications Union, up to 2004, there were approximately 772 million personal computers in use in the world (GeoHive 2006). It means that practically thirteen percent of the world population are PC users (ibid.).
- While the Internet has expanded into 214 countries and world regions, the worldwide Internet users have been increasing fast in the past ten years. The Internet users reached one billion in 2005, 1.46 billion in 2008, and the growth rate is still high (Internetworldstats.com 2008).

Increase in the number of web sites

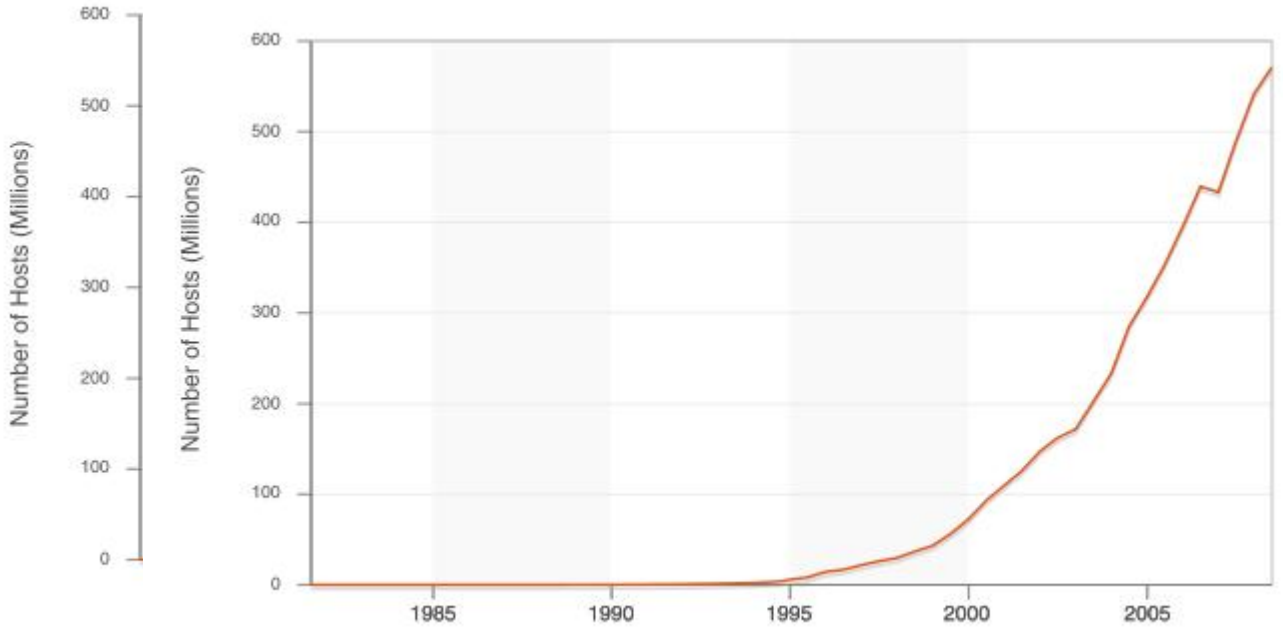
- Representing the number of cyber actors, the quantity of cyber resources, the range of services that users can consume, and the number of places that the potential customers can visit.
- A Netcraft survey in Nov. 2008 found that there were more than 186 million web sites on the Internet. From the increasing process of the Internet domain names worldwide, an accelerated ratio of increase can be discovered from the late 1990s.

Total Sites Across All Domains August 1995 - November 2008



Number of Internet hosts

- The third indicator is the number of Internet hosts.
- As of July 2006, the number of Internet hosts reached 439 million (Internet System Consortium, ISC 2006). From the ISC (2006), the development of Internet hosts from 1969 to 2006 showed that the development was relatively slow in the first two and a half decades, and began to accelerate from the mid-1990s.



- Source: Swivel 2008

Number of web pages

- The fourth indicator is the number of web pages.
- As of 2007, the Google search engine collected 8 billion of web sites, indexed nearly 10 billion of distinct web pages, several billion of all types of images: photos, drawings, paintings, sketches, cartoons, posters, and more. See Google.com's self-description (Chinese version. There may be no such description in versions of other languages).

Bandwidth growth

- The fifth indicator is bandwidth growth.
- Bandwidth growth facilitates more users and more convenient online activities. The lowered cost and enhanced quality of services attract people of various ages, different income levels and educational background to join the online community. A longer online time also becomes possible. Therefore, bandwidth growth directly influences the number of online users, the length of online time, and the categories of online activities.

Internet connection bandwidths

- 56 kbit/s Modem / Dialup
- 1.544 Mbit/s T1
- 10 Mbit/s Ethernet
- 11 Mbit/s Wireless 802.11b
- 43.232 Mbit/s T3
- 54 Mbit/s Wireless-G 802.11g
- 100 Mbit/s Fast Ethernet
- 155 Mbit/s OC3
- 300 Mbit/s Wireless-N 802.11n
- 622 Mbit/s OC12
- 1000 Mbit/s Gigabit Ethernet
- 2.5 Gbit/s OC48
- 9.6 Gbit/s OC192
- 10 Gbit/s 10 Gigabit Ethernet
- Source: http://en.wikipedia.org/wiki/Bandwidth_(computing)

Growth of scale of e-commerce

- The sixth indicator is the growth of scale of e-commerce.
- In the U. S. alone, five years after the introduction of the WWW, the size of Internet economy can compete with traditional sectors, such as energy, automobiles, and telecommunications (Centre for Research in Electronic Commerce 1999, p. 8). The Internet economy also rewrote the history of the employment market (Ibid, p. 9).

Uncontrollability of networked activities

- The universal accessibility of the Internet
- The invisibility of cyberspace
- The low controllability of the process
- The disputability of content and activities
- The divisibility of digital files
- The low confidentiality of information systems
- Anonymity
- The abuse of services
- From information society to mobile society: the uncertainty of the future

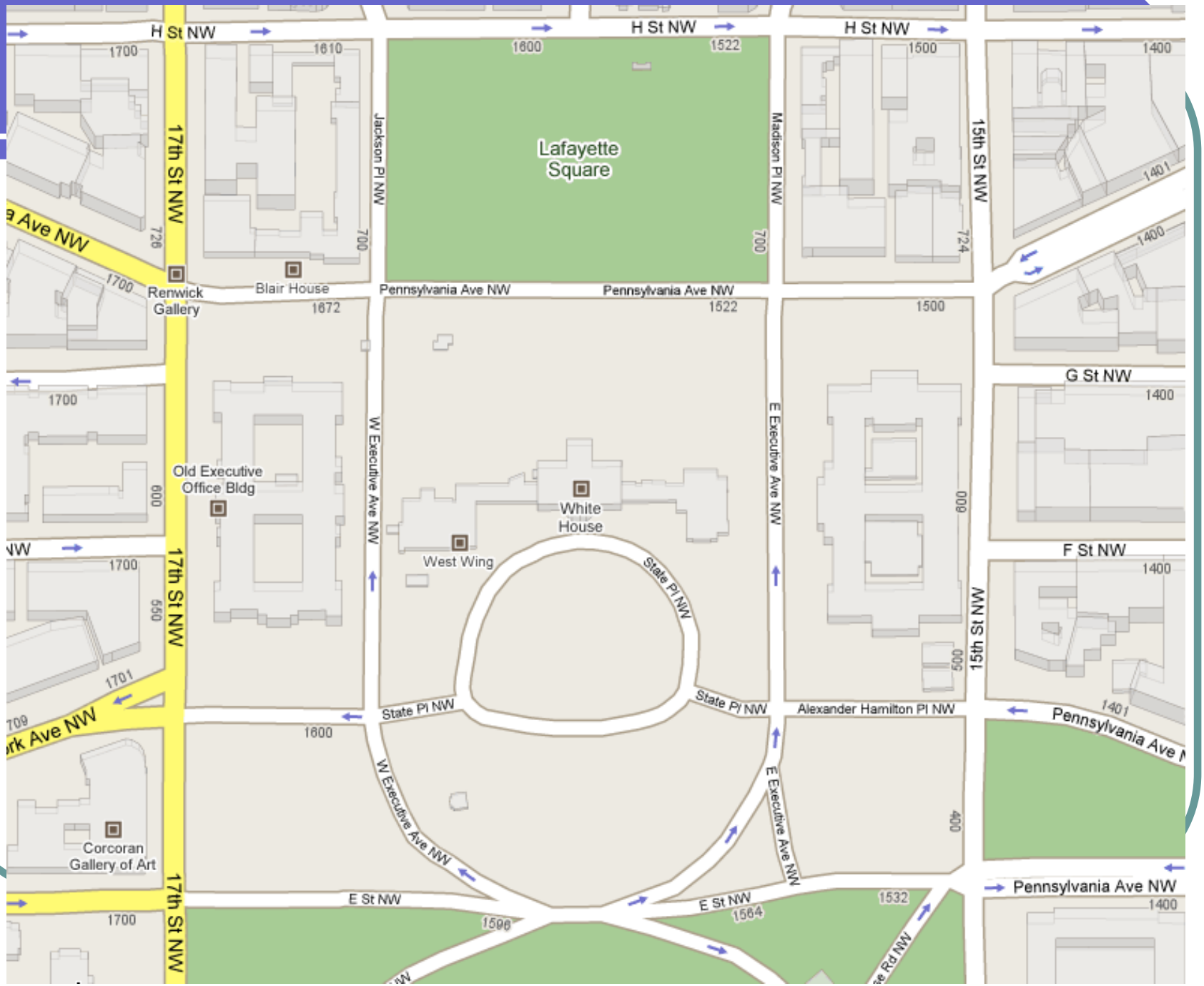
The universal accessibility of the Internet

- The case of Cyber cafés

- Jinan city, Julong cyber café, 5688 sqm, 1777 computers
- Source: http://www.xayesky.com/article/2007/0901/article_22148.html

The invisibility of cyberspace

- The case of Internet address: White House offline and White House online
- Where is http://www.whitehouse.gov/?


H St NW
1700
1610
1600
1522
1500
1400
17th St NW
Jackson Pl NW
Madison Pl NW
15th St NW
Lafayette Square
Renwick Gallery
Blair House
Pennsylvania Ave NW
1672
726
700
724
1401
G St NW
Old Executive Office Bldg
W Executive Ave NW
E Executive Ave NW
White House
West Wing
State Pl NW
Alexander Hamilton Pl NW
600
500
F St NW
1701
709
660
Corcoran Gallery of Art
E St NW
1600
1590
1564
1532
400

from PERIL to PROGRESS

In his first two Presidential Memoranda, President Obama took two bold steps on the journey towards energy independence.

READ the PRESIDENT'S REMARKS

MORE FEATURES:

1 2 3 4

THE BLOG

MORE FROM THE BLOG

TUE, JANUARY 27, 5:50 PM EST

Sec. Geithner tightens the reins

In one of his first acts as Secretary of the Treasury, Timothy Geithner today announced new rules that will make it harder for banks to lobby for a share of money set aside by the Emergency Economic Stabilization Act.

READ THIS POST

TUE, JANUARY 27, 2:01 PM EST

On the Hill

President Obama is on Capitol Hill today to hear out

SEARCH THE SITE

SEARCH

AGENDA

Economy

Read the President's economic agenda.

Energy & the Environment

Read the President's agenda on energy & the environment.

WHISTLESTOP TRAIN TOUR

The low controllability of the process

- The case of online forum

- Right to censor or control?
- Energy and time for control?

The disputability of content and activities

- The case of free speech
- Can be translated into a question: how free is speech?

Welcome Guest (Log In | Register)

Groundspeak
The Language of Location

Niche Geocaching Products Most €80k+ Jobs in Eur
Camo labels, bags, micros, pens & Executive Career Service Ne
Ads by

Visit Geocaching.com Read the Forum Guidelines Help Search Members Cal

Groundspeak Forums > Geocaching Groups by Country > United Kingdom

95 Pages 1 2 3 > »

ADDREPLY

The All New All New Groundspeak UK Pub Quiz, Off topic - but lets see how it goes...

Option

Simply Paul — Mar 31 2007, 10:54 AM

I'm dreaming of a green giftmas

Group: Premium Members
Posts: 4,429
Joined: 25-May 03
From: Aylesbury, Bucks, UK

As the other quiz thread was closed 'in mysterious circumstances', the question from SlytherinAlex was "Who/what is the photographed person/object in the world. Each day - every day."

Dorsetgal & GeoDog (but mostly Dorsetgal) suggested the Statue of Liberty. Of which there are many...

Quickie edit: The original thread is here

This post has been edited by **Simply Paul**: Mar 31 2007, 10:56 AM

OFF CARD PM TOP QUOTE

scaw — Mar 31 2007, 10:58 AM

Princess Diana?

Who/what is the most photographed person/object in the world. Each day – every day?

- Princess Diana
- Great wall of China
- George Bush
- Camera lenses
- Eiffel Tower
- The Sky
- The photographer's finger
- The lenscap
- An x-ray table
- Light
- Naked Women
- Dust
- The moon
- Mankind
- Baby
- The President of the U.S.A.
- Family and friends
- Elizabeth Alexandra Mary Saxe-Coburg Gotha, aka Battenburg, aka Betty Windsor
- Mickey Mouse
- Themselves outside their house
- Mountain Thistle
- ...

The divisibility of digital files

- The case of control over piracy

The Pirate Bay

Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100

Preferences
Languages

All Audio Video Applications Games Other (search titles only)

Pirate Search | I'm Feeling Lucky

How do I download?

Login | Register | Language / Select language | About | Legal threats | Blog
Contact us | Usage policy | Calendar | Doodles | Search Cloud | Tag Cloud | Forum | **TPB T-shirts**
SlopsBox | BayWords | BayImg

3,239,869 registered users. Last updated 08:22:04.
21,004,993 peers (8,418,246 seeders + 12,586,747 leechers) in 1,436,445 torrents on tracker.

- **Legal threats against The Pirate Bay**
- Microsoft: email (we get tons of these)
- Mono Music: email (swedish)
- DreamWorks: email our response
- EA: email our response
- Uppsala universitet: emails our response mail exchange back and forth final mail (they also called the phone# in whois) (swedish)
- ADV Films: email our response
- Sublimal Sounds: email our response 2nd mail and response
- SEGA: email our response 2nd mail 3rd mail and response
- Sveriges Radio: email our response (swedish)
- Peter Pehrson - enya.com / Warner Music: email our response
- Apple: email our response
- White Stripes / WEB SHERIFF: email our response 2nd mail and response our fax (invoice) 3rd mail attached document We tell Faxxsheriff about our new site 4th mail our response
- Warner Bros / Billy Corgan / GrayZone Inc: email our response
- Warner Bros / Disturbed / GrayZone Inc: email our response 2nd email and response
- iRacing: letter (yes, they sent us a PDF) our response (the actual response was a 1MB BMP file, but well...)
- Andrew Rabbitt / Rabbit Valley Comics: email our response 2nd email
- Linotype: postal mail (1 2) our response (1 2)
- Prophecy House: email and our response (he also called us, talking about the antichrist)
- MPAA / Hollywood / Swedish goverment / a lot of people (2006-05-31): MPAA press release our comment
  Most of you probably know of the big raid of 2006-05-31. Some day we will write a separate page about all the events. Look at the documentary Steal This Film for more information.
- Indiana Gregg (Gr8pop ltd) (2008-06-22): email and response, 2nd email and response, 3rd email and response, 4th (sic!) email and response
- No action (except ridiculing the senders) has been taken by us because of these. :-)
- **Nice graphs for the law firms who don't get the hint above:**
- (we used to have a nice graph here, but it's simpler to just say: 0 torrents has been removed, and 0 torrents will ever be removed.)
- Source: The Pirate Bay, 2008

20 February 2004

Dear Sir or Madam,

This letter serves as notification under the Digital Millennium Copyright Act, 17 U.S.C. § 512, or equivalent notice provisions of your local law, that content currently residing within your computer system infringes on the copyrights of Microsoft Corporation. Moreover, the source code contains proprietary trade secret information belonging to Microsoft. I am authorized to act on behalf of Microsoft in this matter.

The infringing material residing on your system is the source code for Windows 1998, Windows NT, and/or Windows 2000. This source code, copyrighted by and proprietary to Microsoft, is on your system at the following location:

http://tracker.piratbyran.org/torrents-details.php?id=2614,
http://tracker.piratbyran.org/torrents-details.php?id=2959,
http://tracker.piratbyran.org/, http://www.piratbyran.org/
Posting of Microsoft's source code as described above is not authorized by Microsoft, any of its agents, or by law. Pursuant to this notification, you should immediately take steps to locate and remove and/or disable access to the Microsoft source code that is on your system at the web address detailed above. As a service provider, you may otherwise be liable for copyright infringement if, upon obtaining knowledge or awareness of infringing material being stored upon your network, you do not act expeditiously to remove, or disable access to, the material. 17 U.S.C. § 512(c).

The information in this notification is accurate. I swear under penalty of perjury that I am authorized to act on behalf of Microsoft in regard to its exclusive rights in the work(s) identified above that I believe has been and continues to be infringed as described above.

We hereby give notice of these activities to you and request that you take expeditious action to remove or disable access to the material described above, and thereby prevent the illegal reproduction and distribution of this source code via your company's network.

We appreciate your cooperation in this matter. Please advise us regarding what actions you take.

Yours sincerely,

James Young
Internet Investigator

Source: http://static.thepiratebay.org/ms-loveletter.txt

The low confidentiality of information systems

- USA v. Devon Lynn Townsend: During 11 months, the defendant from New Mexico used an interactive computer service, and a facility of interstate commerce to engage in a course of conduct that caused substantial emotional distress to Mr. and Mrs. Chester and Talinda Bennington in California (pp. 5-6). Over the course of several months, the defendant was able to access all sorts of private information about the Benningtons from their private e-mail accounts, including:
- "(a) family pictures of the Benningtons and their minor children;
- (b) correspondence between Wamer Brothers Records and the business attorney for Linkin Park, including a copy of a check made payable to Chester Bennington from the record company as well as a copy of the recording contract between Wamer Brothers Records and the members of Linkin Park;

- (c) information about a new home purchase by the Benningtons which included such documents as a home inspection report, images of the home's interior, and other real estate documents;
- (d) information about the Benningtons' travel plans including flight information and the name of motels and hotels where the Benningtons had reservations;
- (e) a copy of a dental bill for Talinda Bennington;
- (f) information about the time and location of Mrs. Bennington's childbirth classes;
- (g) e-mail correspondence concerning the whereabouts and after school activities of the Benningtons' child;
- (h) information about purchases the Benningtons made for their newborn child;
- (i) information about the schedule and itinerary of the members of Linkin Park, including their itinerary for the Grammy awards show in 2006" (pp. 7-8).

Anonymity

- The case of cybertalking
- The real identity of the user is not necessary for using the Internet. In the environment of online communications, particularly during interaction between remote strangers, information systems provide the possibility of maintaining anonymity, and we found that the users of information systems have the willingness to stay passively anonymous, not necessarily actively lying to their counterparts (Li 2008, pp. 103-105)

- **The Internet makes stalking different**: Internet services, such as e-mails, are also abused by cyberstalkers to send text-, graphic-, audio- and video-based messages to the e-mail account of the intended victim, transmitting the content of threatening, alarming, or harassing (D'Ovidio and Doyle 2003, pp. 10-17).

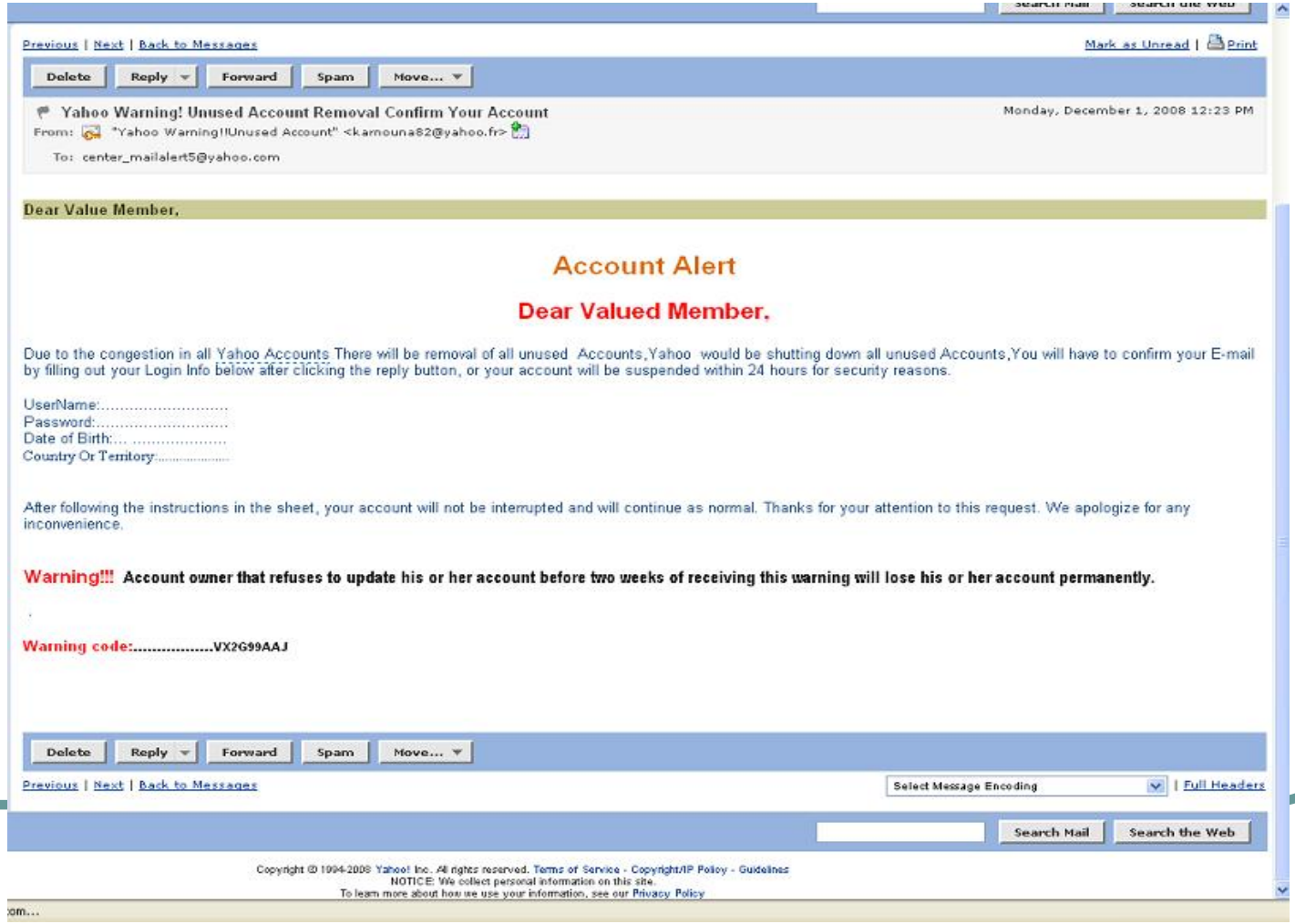
- In Cullen v White [2003] WASC 153, the defendant originally published a number of postings in a discussion forum on the World Wide Web, disparaging of a university where the plaintiff once worked and a number of people whom the plaintiff had known there. After the plaintiff had known this, he wrote to the webmaster to urge him to remove the postings. The webmaster published the plaintiff's letter on the discussion forum web page. Within days the university where the plaintiff was then studying, began to receive e-mails from the defendant claiming that the plaintiff was a fraud. Within two months, the defendant had created a web site for his attacks on the plaintiff.

USA v. Erik Bowker

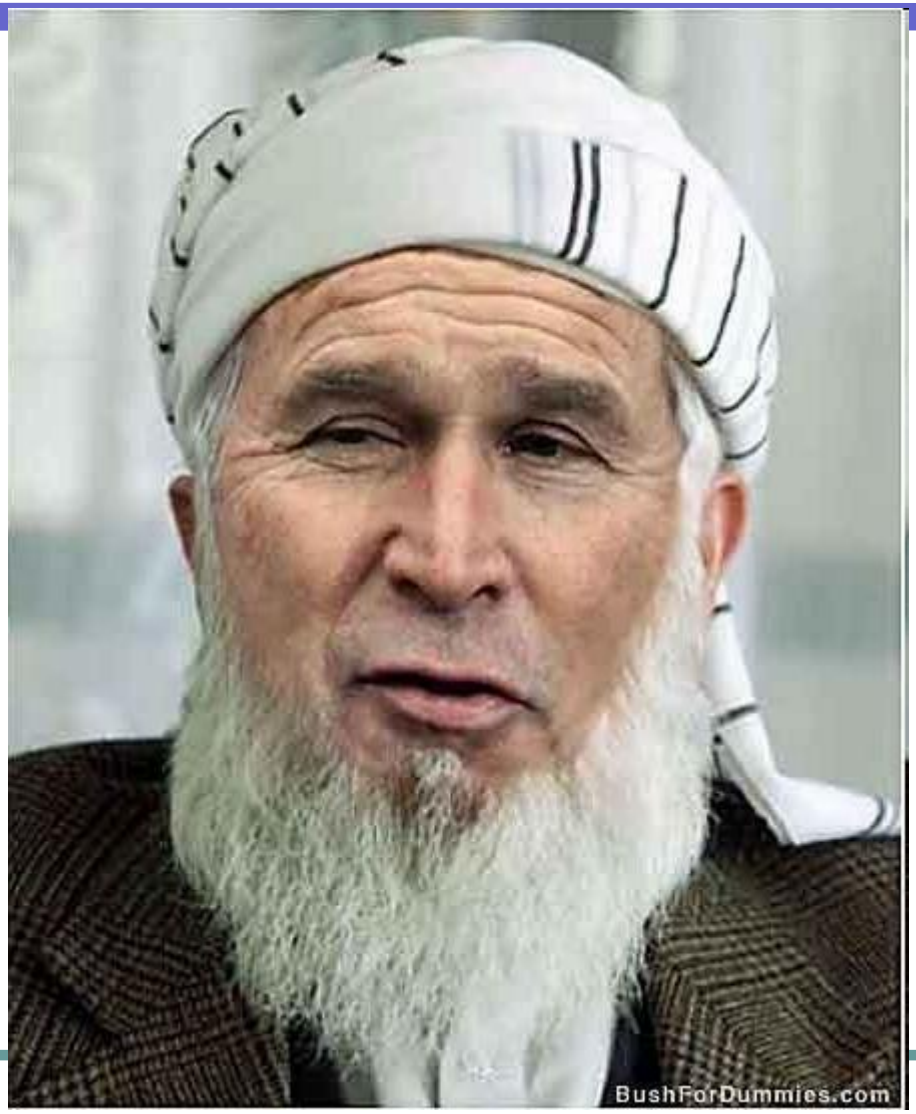
- During over one year, the stalker sent a number of emails full of verbal threats relating to the victim. The emails were sent from several different email addresses and purported to be from an individual variously identified. After an FBI Special Agent sent emails to the various email addresses on the correspondence pertaining to the victim, the victim began receiving hand-written notes from a person of different identity almost every couple of days. Even worse, after the victim more to a new location, the stalker, with different identities, sent the victim a card saying that his letters to her were all online in a mail account at yahoo.com. The stalker also continued to attempt telephone contact with the victim, 146 telephone calls from his cell phone to where the victim worked and 16 calls to the victim's personal residential telephone. Knight's number was unlisted and unpublished. While the stalking was continuous and obsessive, the identity of the stalker reserved changed and concealed, taking FBI agent several months to trace back.

Abuse of services

- The case of spam


Previous | Next | Back to Messages
Mark as Unread | Print
Delete
Reply
Forward
Spam
Move...
Yahoo Warning! Unused Account Removal Confirm Your Account
Monday, December 1, 2008 12:23 PM
From: "Yahoo Warning!!Unused Account" <karnouna82@yahoo.fr>
To: center_mailalert5@yahoo.com
Dear Value Member,
Account Alert
Dear Valued Member,
Due to the congestion in all Yahoo Accounts There will be removal of all unused Accounts,Yahoo would be shutting down all unused Accounts,You will have to confirm your E-mail by filling out your Login Info below after clicking the reply button, or your account will be suspended within 24 hours for security reasons.
UserName:.....
Password:.....
Date of Birth:... .....
Country Or Territory:.....
After following the instructions in the sheet, your account will not be interrupted and will continue as normal. Thanks for your attention to this request. We apologize for any inconvenience.
Warning!!! Account owner that refuses to update his or her account before two weeks of receiving this warning will lose his or her account permanently.
Warning code:.....VX2G99AAJ
Delete
Reply
Forward
Spam
Move...
Previous | Next | Back to Messages
Select Message Encoding
Full Headers
Search Mail
Search the Web
Copyright © 1994-2008 Yahoo! Inc. All rights reserved. Terms of Service - Copyright/IP Policy - Guidelines
NOTICE: We collect personal information on this site.
To learn more about how we use your information, see our Privacy Policy

Bush Laden? (Google picture search)



Defaced White House (BBC, May 2, 2001)

- Video: “How to Hack a Website in 50 Seconds…”
- at http://www.youtube.com/watch?v=c8uw6yU2vfU

- Video: “How to Make a Trojan Virus in less than 3 Minutes”

at

http://www.youtube.com/watch?v=YX4P-KS-j6c&feature=related

- Skip “Terrorist manual”, at

http://www.fas.org/irp/world/para/aqmanual.pdf

Conclusion

- Firstly, the objects requiring the protection of the criminal law have been expanded in the information age.
- Secondly, because of the expansion of the objects to be protected in the criminal law, it is very important to provide definition of new types of crimes, and to revise constituent elements of old crimes, in which information systems become a new tool, object, place, medium, route, and means of traditional offences.
- Thirdly, the space of criminal justice is expanding beyond traditional society.
- (to be continued)

- Fourthly, balance has not been reached between the influence of technology on criminal justice and on criminal phenomena, both of which are complex and involve positive and negative forces.
- Fifthly, the dependence of criminal law on technology, and the interaction and mutual support between criminal law and technology should reach an unprecedented extent. Without the interaction of technology, criminal law could not obtain so great a deterrent effect.

References

- Centre for Research in Electronic Commerce. 1999. Measuring the Internet Economy, The University of Texas at Austin.
- D'Ovidio, R., and Doyle, J. 2003. A Study on Cyberstalking: Understanding Investigative Hurdles, The FBI Law Enforcement Bulletin, volume 72, pp. 10-17.
- GeoHive. 2006. Countries with Most Personal Computers. Retrieved 15 March 2007, from http://www.geohive.com/charts/charts.php?xml=ec_inet&xsl=ec_inet_top2
- Internet System Consortium (ISC). 2006. Internet Domain Survey. Retrieved 15 March 2007, from http://www.isc.org/index.pl?/ops/ds
- Internetworldstats.com. 2007. Internet Usage Statistics-The Big Picture. Retrieved 27 July 2007, from http://www.internetworldstats.com/stats.htm.
- Li, X. 2008. Cybercrime and Deterrence, Uniprint.

- Any questions?

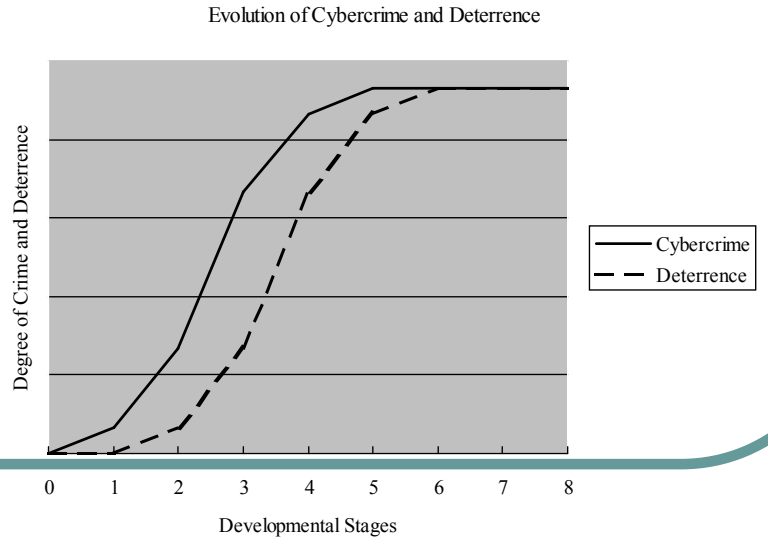
Cybercriminology Lifecycle of Cybercrime

Xingan Li, LLD
Faculty of Law
University of Turku

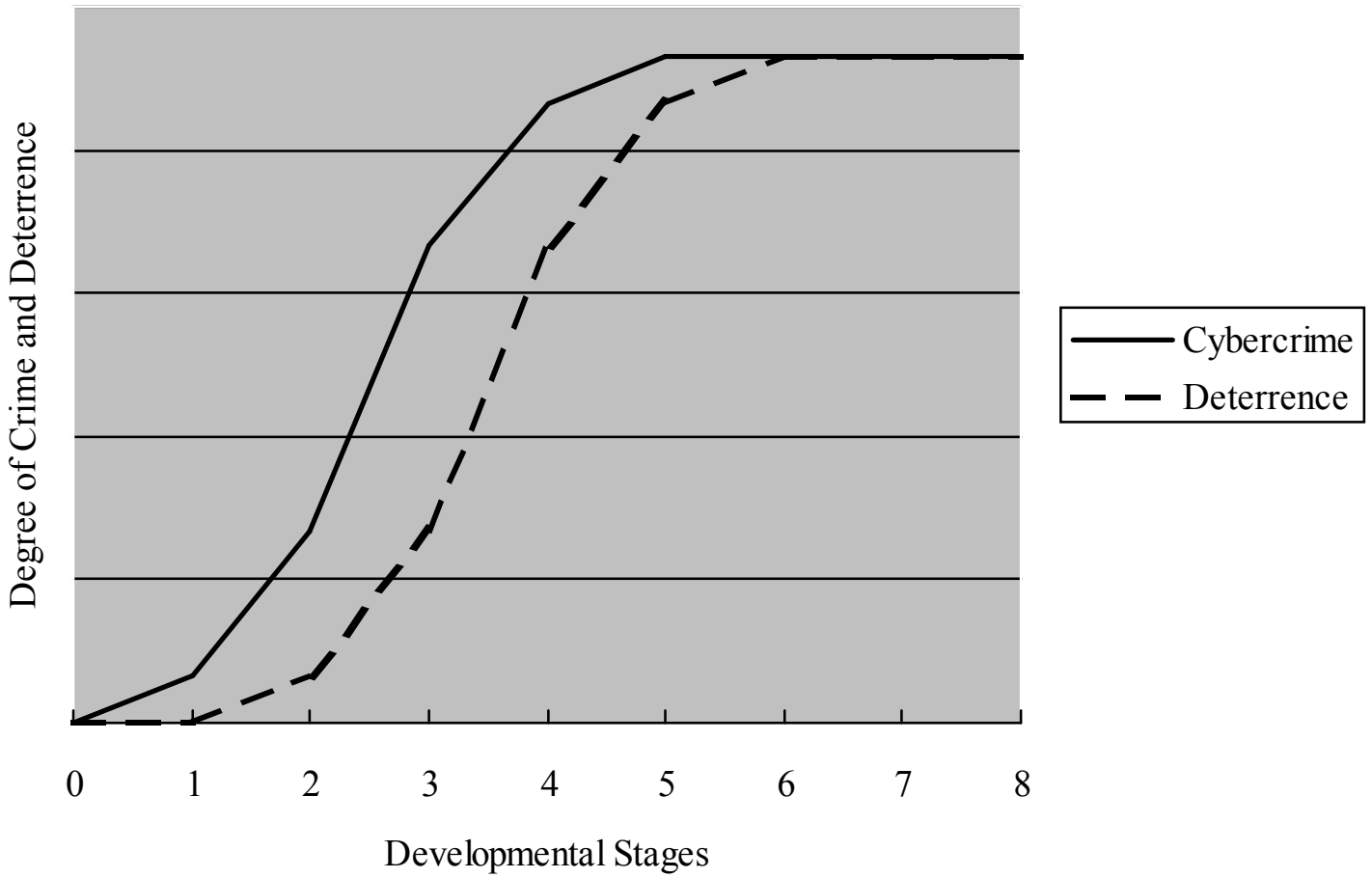
DOI: 10.13140/2.1.4660.0489

UNBALANCED SCALE: THE HISTORICAL DEVELOPMENT OF CYBERCRIME AND DETERRENCE

- Basic observations on the development of criminal phenomena
- "History is full of nightmares, some natural, some manmade." –Clarke 1997, p. 223.

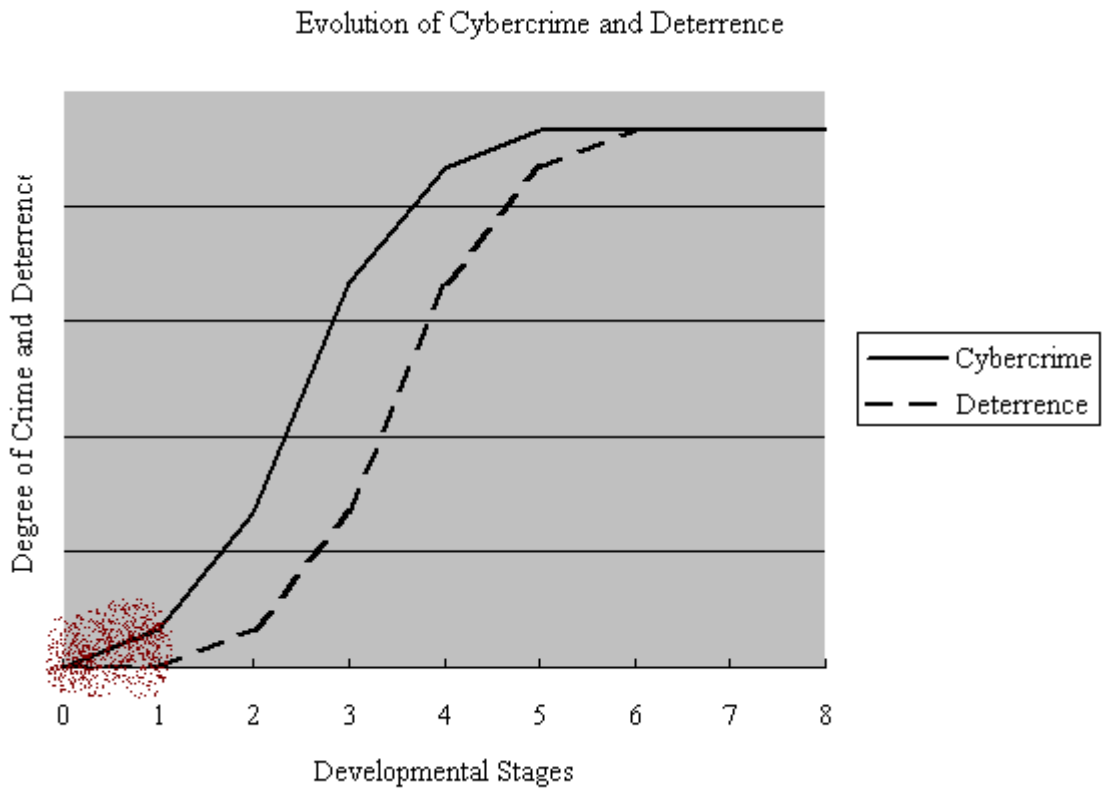


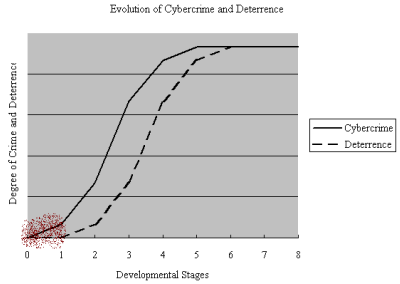
Evolution of Cybercrime and Deterrence



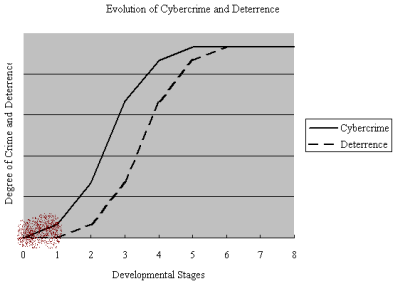
- Cybercriminal phenomena and the deterrence of punishment through law enforcement and social prevention are undergoing a process of development.
- The history of cybercrime can roughly be divided into four stages: a stage of germination, a stage of rapid development, a stage of broad expansion, and a stage of routinization. Furthermore, the criminal-law reform relating to cybercrime has never been completely synchronous with cybercrime due to a hysteresis in both the law enforcement and legislation compared with the relevant criminal phenomena.

Computer hackers' discovery of a lawless new frontier 1940s-1960s



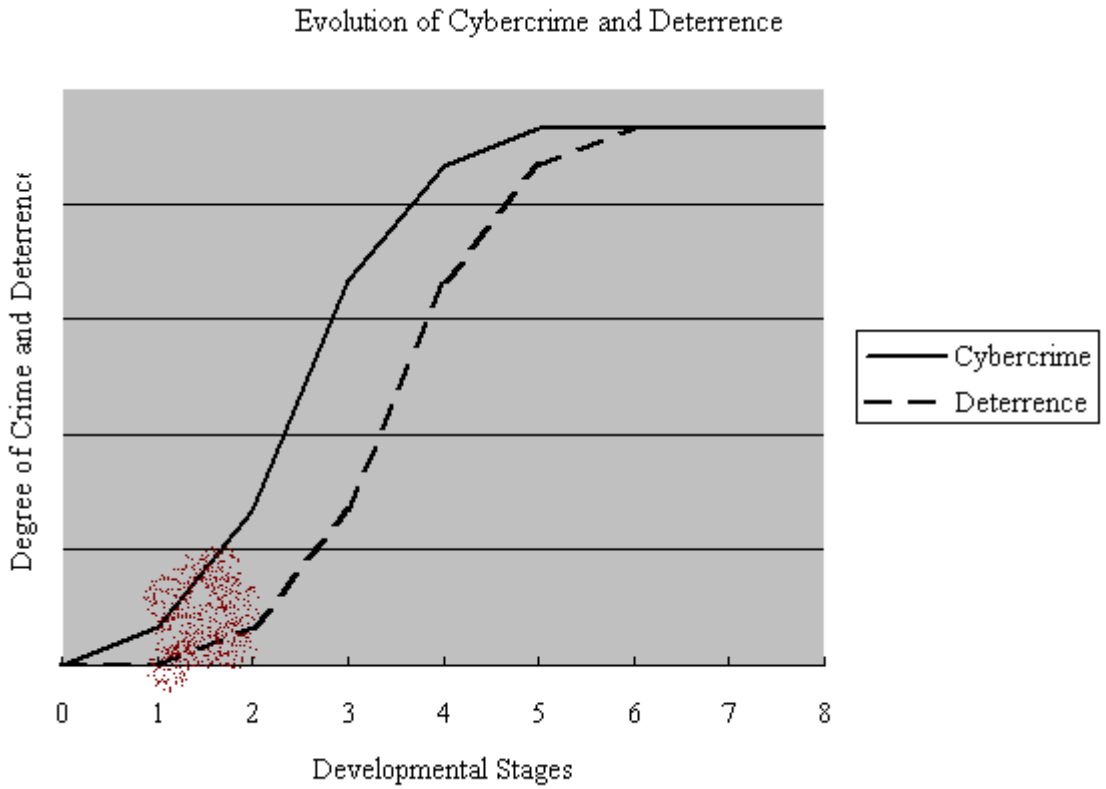


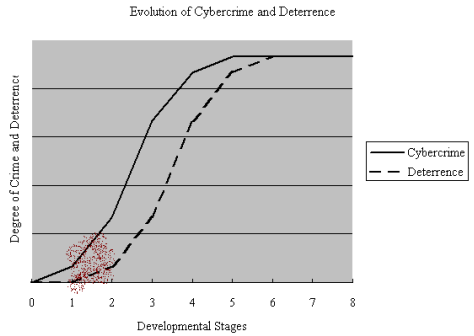
- Computer crime emerged soon after the invention of the first computers
- General public paid more attentions to usability, utility, efficiency, and development of the computer
- The manufacture or installation of a computer is an expensive and time-consuming work, but computers increased from 400 to 60,000.
- Computer crime occurred in the context of a limited number of computers in use
- Cold War's product: ARPANET
- Legislature did not provide any specific countermeasures against the phenomenon



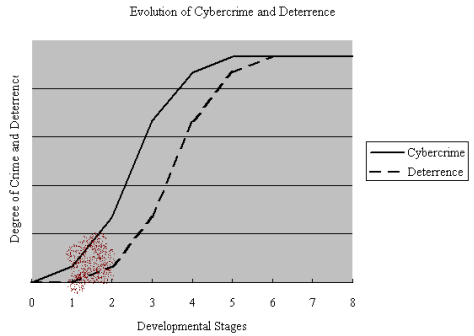
- Time lag between occurrence and prosecution of the first computer crime, 8 years
- Hacker culture originated from scarcity of the computer. Hacking for free use…

The rise of the law against the increasing number of cybercrimes 1970s-1980s

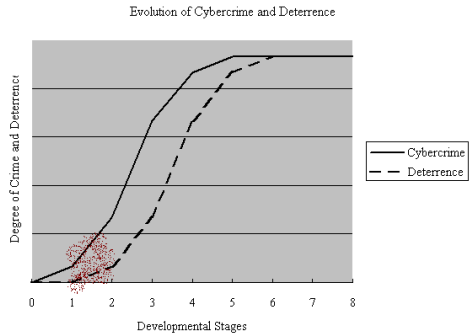




- Increasing dependence on the computer
- "The computer would be growing in power while withdrawing as a presence." (Mosco 2004, p. 21)
- Information revolution, post-industrial society (Bell 1974), information age, information society…
- "Cyberspace" coined by novelist Gibson (1984)
- Trojan Horse, virus, worm, logic bomb came into being in 1970s and 1980s



- Computer crime diversified: vandalism, theft of information, theft of services, theft of property, and fraud (Bequai 1979). Besides viruses, there were also fraud and other abuse of computer, software theft, and piracy.
- Law and law enforcement still insufficient. However, a certain degree of deterrence began to exist, but not effective enough.

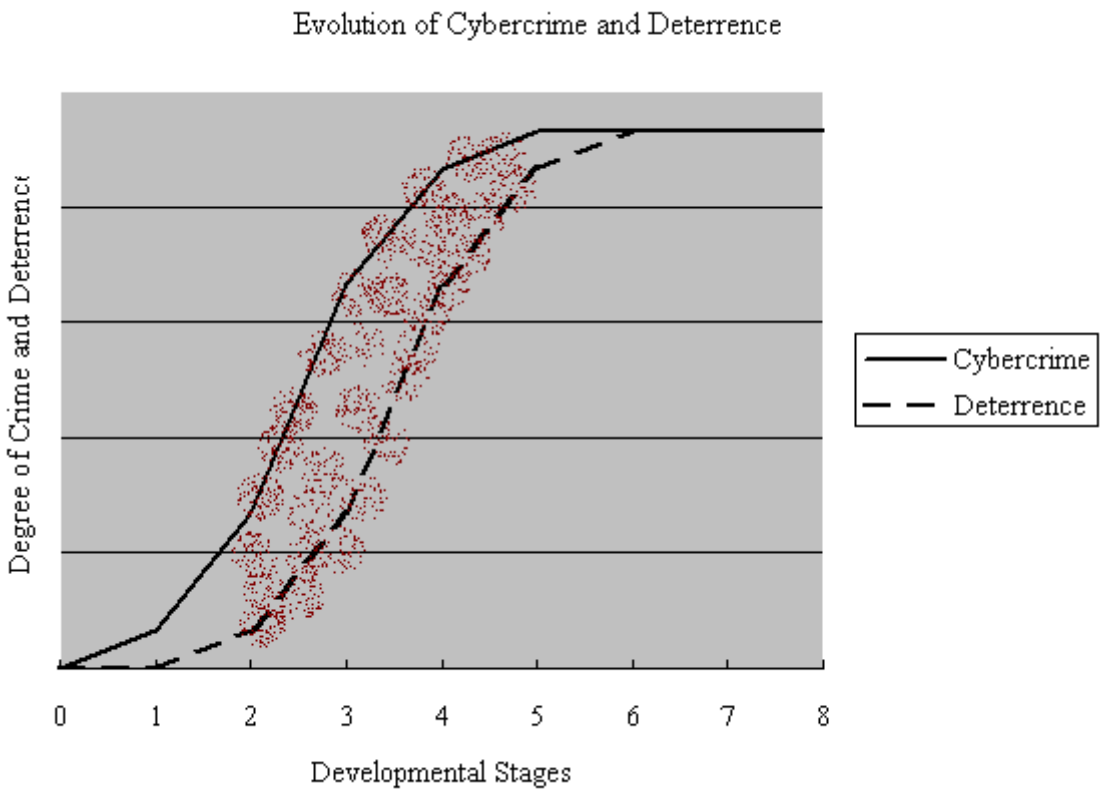


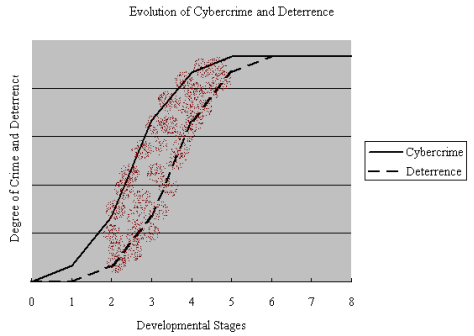
- Borrowing Gary Becker's (1968) analysis:

- Risk-indifferent: indifferent to detection and conviction
- Risk-lovers: new cause, new chance, new challenge, new risk
- Risk-avoiders: low risk of detection and conviction rate of cybercrime, transferring from other offences to cybercrime

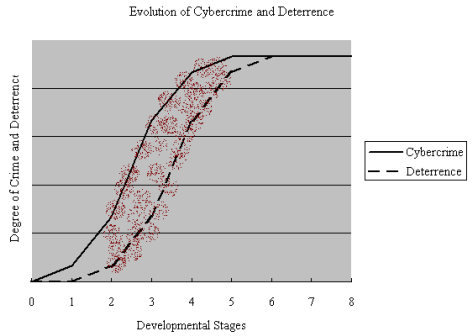
- Enlarged gap between crime and deterrence

A legal system wrestling with networked adversaries 1900s

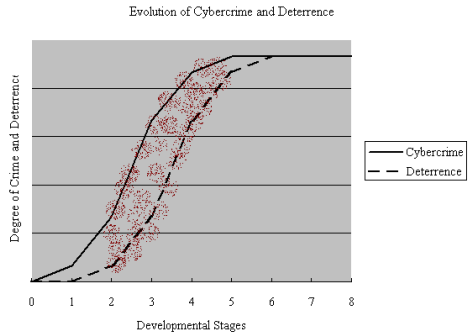




- "Today, we are witnessing the early turbulent days of a revolution…A new medium of human communications is emerging, one that may prove able to surpass all previous revolutions…in its impact on our economic and social life." (Tapscott 1996, p. xiii)

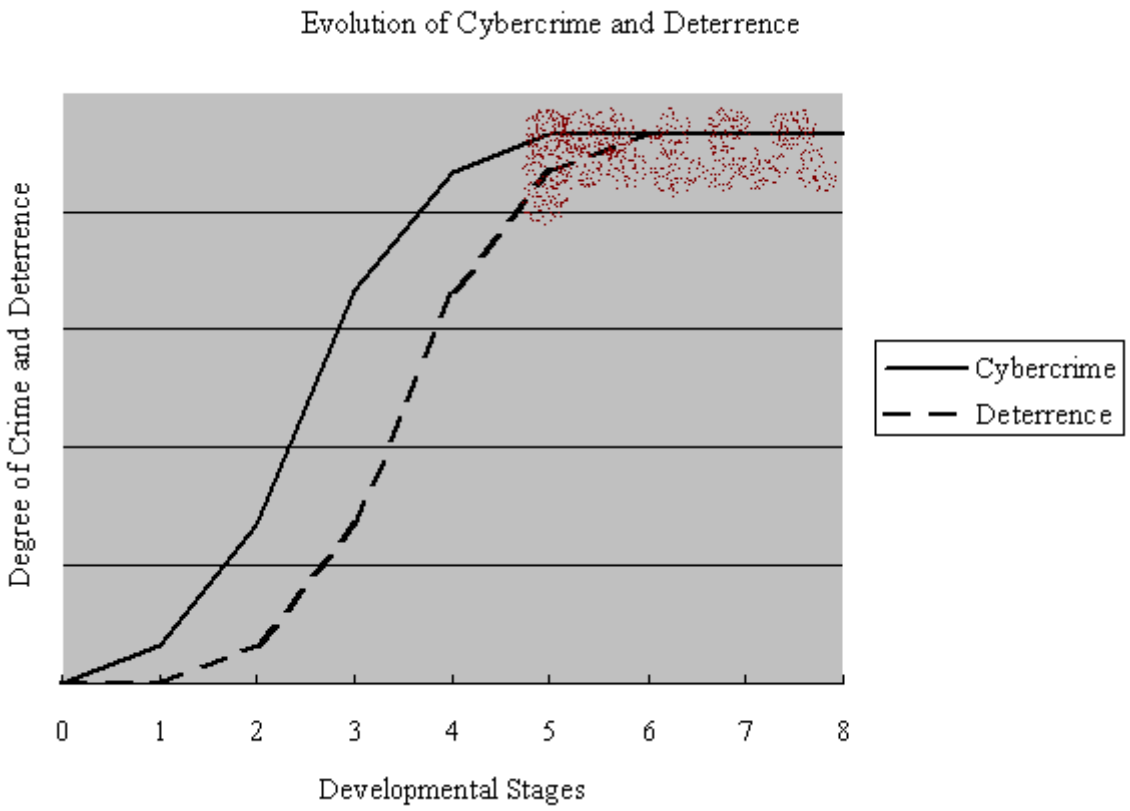


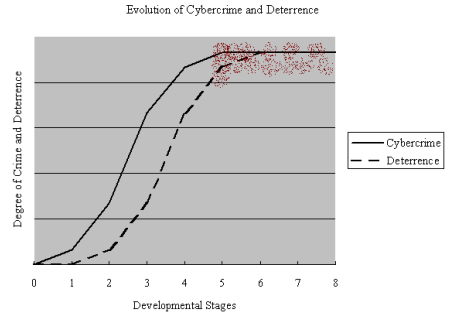
- The open access of the Internet to the commercial use from early 1990s
- The introduction of the concept of National Information Infrastructure
- The invention of World Wide Web



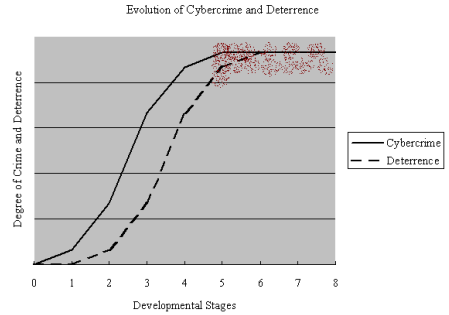
- Globalization of cyberspace, globalization of cybercrime
- Privacy, defacement, spam, infringement of intellectual property
- Asian Financial Crisis
- Legislation, and crackdown: shrank gap between crime and deterrence

The equilibrium between cybercrime and deterrence 2000s-



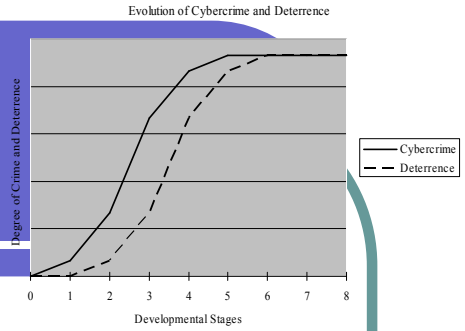


- Breakdown of network economy boom in 2000
- Large-scale Denial of Services attack
- Advance-fee fraud
- Defacement
- Number of cases fell since 2001
- Law in developing countries made



- 911
- …and cyberterrorism, never happened
- Not so much people link today's global financial crisis with cybercrime or cybersecurity

Conclusion

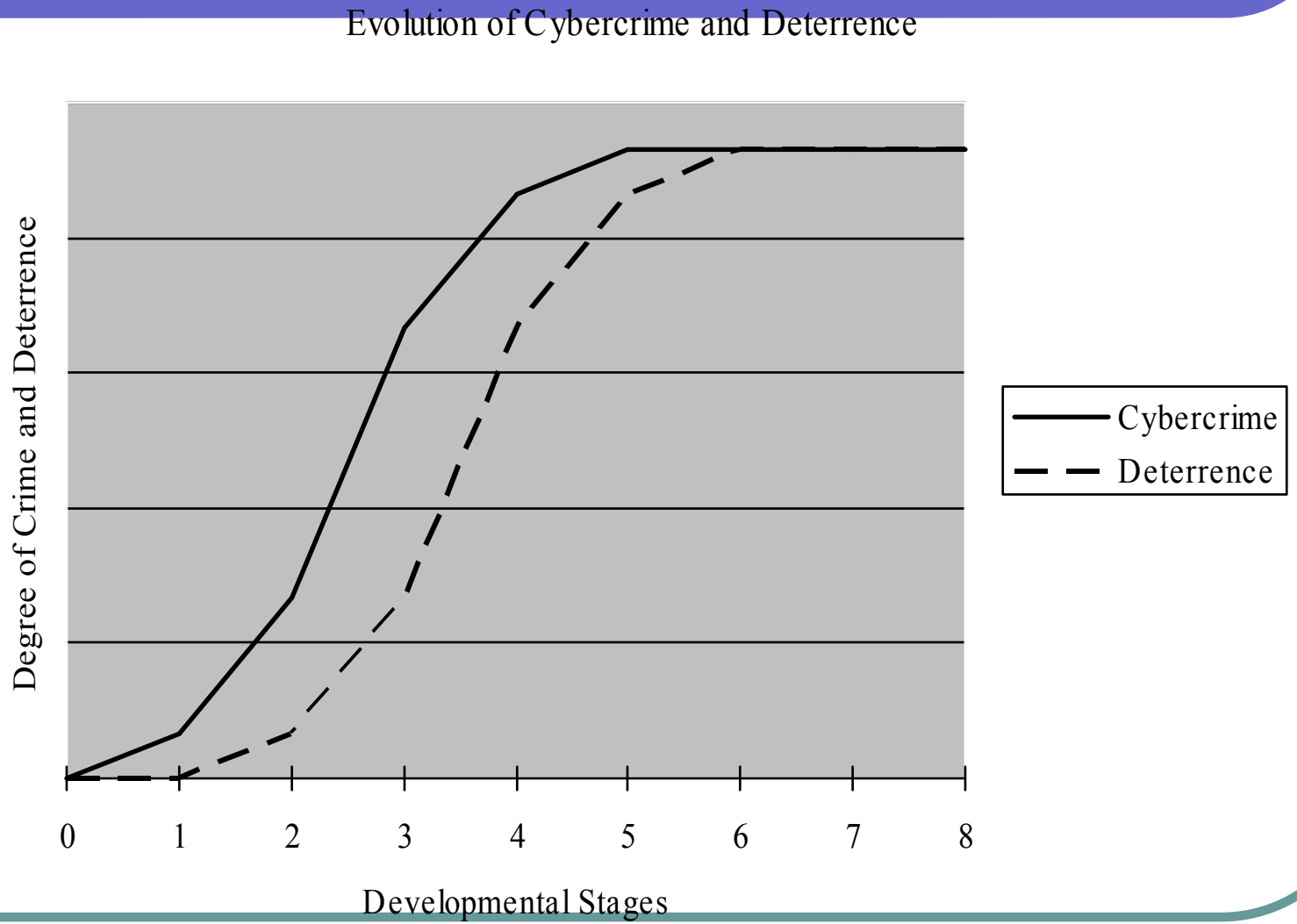


- Limits of crime resources criminal productivity and deterrence resources and deterrence productivity
- Y axis: increase tendency of crime and deterrence
- X axis: developmental stages
- From Point 0 to Point 1: the first stage, cybercrime without deterrence, developing slowly.
- From Point 1 to Point 2: the second stage, cybercrime with initial deterrence, developing faster.
- From Point 2 to Point 5: the third stage, cybercrime with gradually strengthened deterrence, the development tendency is the fastest and then slows down.
- After Point 5: the fourth stage, cybercrime with the strongest deterrence, routinised, saturated, and balanced with deterrence. Cybercrime might sometimes increase, sometimes decrease, but the number and losses would be relatively stable. At this stage, both the level of cybercrime and level of deterrence are subject to limits of each other's resources and productivity.

References

- Clarke, A. C. 1997. *3001: The Final Odyssey*, Hammersmith, London: Voyager.
- Grauer, M. 2001. Information Technology, Information and Knowledge, in N. J. Smelser and P. Bates (eds.). International Encyclopaedia of the Social and Behavioral Sciences, New York, N.Y.: Elsevier, volume 11, 2001, pp. 7475-7476.
- Li, X. *Cybercrime and Deterrence*, Turku: Uniprint, 2008.
- Tapscott, Don. 1996. *The Digital Economy: Promise and Peril in The Age of Networked Intelligence*, McGraw-Hill.
- Tarkhov, S. Generations of the Computers: From Lamp Monsters to Integrated Chips, September 1999. Retrieved 15 March 2007, from http://www.bashedu.ru/konkurs/tarhov/english/generat.htm.

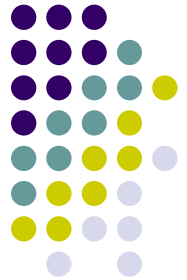
Any questions?



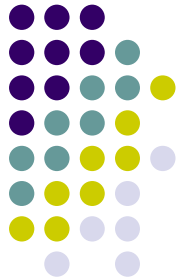
Cybercriminology Hallmarks of Cybercrime

Xingan Li, LLD
Faculty of Law
University of Turku

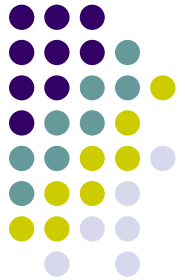
Profile of cybercrime and cybercriminal?



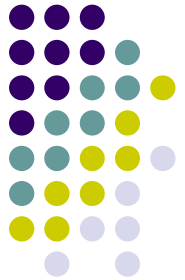
- Bequai (1978, p. 4) presented that:
- “Studies of computer criminals usually portray them as young, educated, technically competent, and usually aggressive. Some steal for personal gain, others for the challenge, and still others because they are pawns in a larger scheme…Still other studies typically portray computer criminals as technicians, managers, and programmers. They are usually perceived as jovially challenging the machine, and discovery occurs only through inadvertence. The theft usually involves money, services, or trade secrets. However, when caught, the computer criminal’s sentence is light compared to that of traditional property-crime felons, who usually receive harsh sentences for crimes involving much less property or money.”



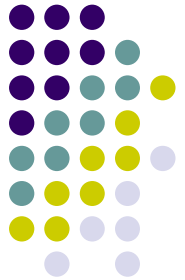
- It has been widely recognised that there is no single profile that can capture the characteristics of a “typical” computer criminal, and many who fit the profile are not necessarily criminals at all (Ware, Pfleeger and Pfleeger 2002, p. 20). Donn B. Parker (1976) has presented a brilliant portrait of a computer crime perpetrator:
- “Perpetrators are usually bright, eager, highly motivated, courageous, adventuresome, and qualified people willing to accept a technical challenge. They have exactly the characteristics that make them highly desirable employees in data processing.”



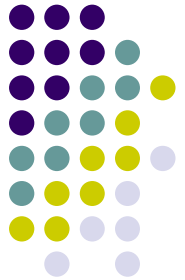
- The development of the computer technology has changed the depiction completely (Becker 1981). Becker (1981) suggested seven views of computer system: the playpen, the land of opportunity, the cookie jar, the war zone, the soapbox, the fairyland, and the toolbox (pp. 18-20).



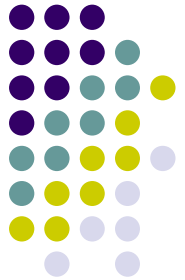
- Bequai (1983, pp. 47-50) researched the potential sources of computer attack might vary from each other, but could be grouped into three categories: dishonest insiders, outsiders, and users. It implied that everyone has an equal chance to be involved in computer crime, in the age when the Internet did not expand as wide as present.



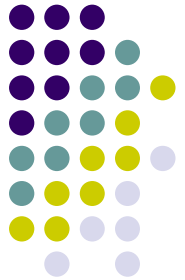
- Wasik (1991, pp. 60-65) concentrated on the characteristics and classifications of perpetrators as well.



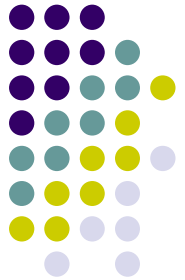
- Levinson (2002) sorted courses of cyber threats into five groups, including insiders, hackers, virus writers, criminals groups, and terrorists (Levinson 2002, p. 525).



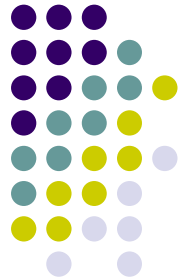
- Reynolds (2003, pp. 58-65) classified perpetrators into hacker, cracker, insider, industrial spy, cybercriminal and cyberterrorist.



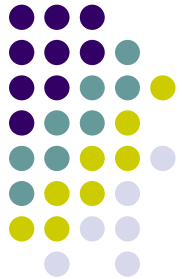
- The Internet users worldwide are strongly sex divided, that is, a higher percentage of males than females use Internet. For example, in 2001, only 6 per cent of Internet users in the Arab States are women; 38 per cent in Latin America; 25 per cent in the EU; 37 per cent in China, 19 per cent in Russia, 18 per cent in Japan, 17 per cent in South Africa, and nearly 50 per cent in the United States are women. However, the distance is increasingly smaller; with females constitute the lager group of Internet users in some countries. In Nordic countries, it was found that also male have a higher percentage of daily users of the Internet (Nordic Council of Ministers 2005, p. 42, Table 2.5).



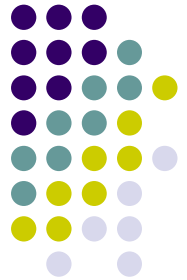
- The previous studies proved that cybercrime is far more sex divided than the Internet use. According to Levinson (2002), “It is well established that boys commit far more juvenile crime, particularly violent crime, than girls.” (p. 490) The cybercrime seems less violent, but the research indicated that more males commit cybercrimes than female.



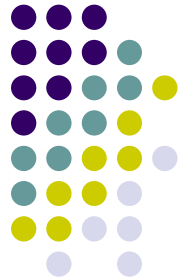
- In individual cybercrimes, corporate cybercrime, or organized cybercrime, the young perpetrators play a critical part. As Shannon (1993, p. 2) reported that, cybercriminals tend to usually be between the ages of 14-30, they are usually bright, eager, highly motivated, adventuresome, and willing to accept technical challenges.
- Juvenile delinquency and juvenile justice became issues closely associated with cybercrime. According to findings of criminal psychological research, the reason why the children are more likely to commit crime is not because more and more children will commit crime, but because most of the potential offenders will commence to commit crime in childhood and continue their criminality for much of their lifetime. After 16-17 years of age, the offending rates decreases to a plateau (Howitt 2002, pp. 76-77).
- Underwood (2002) found that the cybercriminal behaviour cuts across a broad range of society, with the age of most offenders ranging from 10 to 60 years. People between the ages of 20 and 59 make up 94 percent of computer criminals, with the most active being people in their thirties.



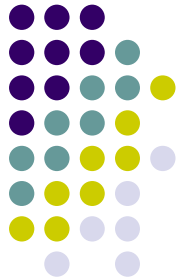
- Bequai (1983, p. 43, Table 1)'s profile of typical computer felon presented a full portrait of the above mentioned aspects, with more other aspects. He stated that the age of computer criminals is between 15-45 years old. Males are responsible for most computer crimes, but females are increasing. The occupational experience of computer criminals differs from the highly experienced technician to a minimally experienced professional. Both public and private sectors could be the victims of the computer crimes. The computer criminals have the personal traits of being bright, motivated, and ready to accept the technical challenge; usually a desirable employee, a hard and committed worker. Computer crimes are mostly by individual perpetrators, but conspiracies are increasing. Most offences are committed by insiders who have easy access to the computer system. The security of the victims' system is usually slack.



- It has been an important topic to distinguish the sources that the offenders come from and the relationship between the offenders and the victims, by which computer crimes can be divided into offences by insiders and offences by outsiders. Shaw, Ruby and Post (1998) classified insiders into information technology specialists such as full-time or part-time employees, contractors, consultants, or temporary workers; partners and customers with system access; and former employees retaining system access. About whether the insiders or the outsiders constitute the greatest threat to the computer system, there have been different findings.

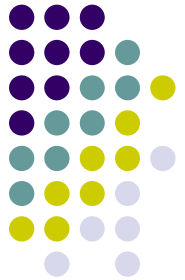


- The mainstream findings support the view that the insiders have been more likely to be involved in computer crimes against the employers' systems. The Nordic Council of Ministers (2005) found that students, employees and self-employed people constitute the higher percentage of the Internet penetration (Nordic Council of Ministers 2005, p. 42, Table 2.5). Mackenizie and Goldman (2000) reported that some students, particularly computer science and engineering majors, with newly discovered skills attempt to break into the servers of University of Delaware (p. 174). Meta Group (2004) found that, of more than 1,600 information and communications technology professionals, current employees represent the biggest threat to technology infrastructures. Computer Security Institute and Federal Bureau of Investigation reported that 55 percent of survey respondents reported malicious activity by insiders (Nelson 2004). Researchers also revealed that the dissatisfied employees are a major source of computer crimes (Vatis 1999) and are the greatest threat to a computer's security (Sinrod and Reilly 2000, pp. 183-187).

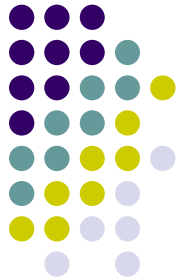


- Besides the revealed relationship between the criminals and victims, others also explored the characteristics of victims. Syngress (2002) summarized the common victim characteristics include those who are new to the Internet; who are naturally naïve; who are disable or disadvantaged; who are greedy, lonely, or have other emotional needs; pseudo-victims who report having been victimized but actually were not; and who are simply unlucky enough to be in the wrong (virtual) place at the wrong time.

My study

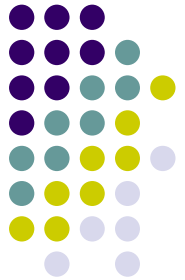


- A sample of 115 reported typical cases sentenced or on trial (during 18 March 1998 to 12 May 2006), published on the web site of the United States Department of Justice. The study took all the cases listed in the web page located at <http://www.cybercrime.gov/cccases.html>
- The study classified the sample cases into hacking and illegal access; attack, sabotage and botnet; viruses, worms, spyware and logic bomb; data theft and espionage; ID theft, fraud; and miscellaneous including embezzlement and corruption.



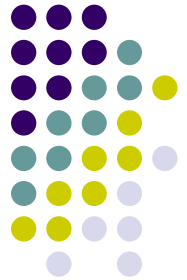
- The statistical items include those related to the demographic characteristics of the cybercriminal (including gender, age, insider or outsider, American citizen or foreigner), the nature of the victims (including private, public, private and public, and public health and safety), the losses of the cases, and the decided punishments on the cybercirme (imprisonment and fine), the guardianship level of the victim (classified into strong, medium, and weak), and the complexities of techniques involved (classified into complicated, medium, and simple).
- The guardianship level and the complexities of techniques are estimated by the process of the crime, the exposing of the vulnerability, criminal-victim relationship, and the availability of the techniques to users.

Gender distribution of cybercrime



- In most categories of offences, male offenders constitute the absolute majority of the criminals. Only two female offenders are reported in hacking and illegal access, one reported in miscellaneous offences (including embezzlement, corruption, and so on). The overall male offenders constitute more than 98 percent of the total perpetrators, while the female are only less than two percent.

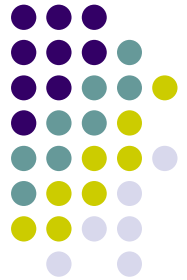
Age distribution of cybercrime



- Three perpetrators younger than 16 years old are convicted with offences in the categories of hacking and illegal access, and viruses, worms, spyware and logic bomb.
- The offenders older than 46 years old distribute in most categories of offences, except fraud and miscellaneous (embezzlement and corruption). However, generally they are not active in computer crime and constitute a small percentage: about 28.6 percent of offenders in data theft and espionage, mote than 9 percent of viruses, worms, spyware and logic bomb, 4 percent of attack and sabotage, and 3.8 percent of ID theft.
- The cyber criminals distribute obviously among the ages between 17 to 45 years old: approximately 79.3 percent of hacking and illegal access, approximately 65.2 percent of attack and sabotage, approximately 63.7 percent of viruses, worms, spyware and logic bomb, approximately 85.8 percent of data theft and espionage, approximately 26.8 percent of ID theft, exactly 100 percent of fraud, and approximately 85.7 percent of miscellaneous (embezzlement and corruption).

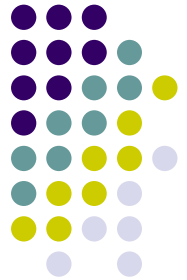
- The ratios of offenders seem to be decreasing with age.

Domestic versus foreign perpetrators



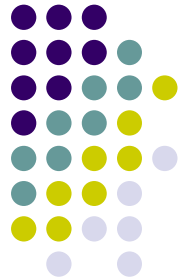
- Altogether 14 out of 115 cases were committed by international perpetrators or foreigners, a ratio of weaker than 12.2 percent. Domestic perpetrators are responsible for the rest 87.8 percent of the cyber criminals. Majority of the reported cases are domestic computer offences.

Insider versus outsider



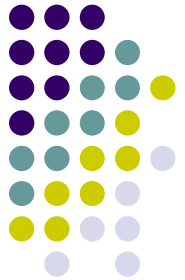
- Insiders and outsiders constitute different ratios in different categories of offences. The categories in which the insiders constitute the majority of offenders include: offenders of data theft and espionage were insiders, while 57.1 percent of fraudsters are insiders.
- The categories in which outsiders constitute the majority of offenders include: exactly 100 percent of ID theft, approximately 92.9 percent of miscellaneous (including embezzlement and corruption), approximately 87 percent of attack and sabotage, approximately 81.8 percent of viruses, worms, spyware and logic bomb, and approximately 76.2 percent of hacking and sabotage. In fact, outsiders also constitute a strong ratio in fraudsters: approximately 42.9 percent.
- The former employees are included in the category of outsiders. A significant ratio of offenders of attack and sabotage are former employees, who constitute approximately 43.5 percent. Former employees also constitute 12.7 percent of offenders of hacking and illegal access, and approximately 7.2 percent of offenders of embezzlement and corruption.
- Overall, insiders and outsiders constitute 21 percent and 79 percent of all reported offenders separately. The former employees constitute 16 percent of all of the outsiders. If add up former employees into insiders, they would constitute about 34 percent of the total offenders, still a less ratio than outsiders.

Losses of cybercrime



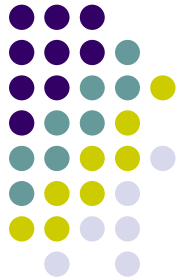
- In more than 59 percent of cybercrime cases, no loss was mentioned in the report. Among the rest less than 41 percent of cases, approximately seven percent are with losses less than 10 thousand dollars, approximately 15.7 percent with losses between 10 thousand and 100 thousand dollars, approximately 10.4 percent with losses between 100 thousand and one million dollars, and approximately 9.6 percent with losses more than one million dollars.
- Hacking and illegal access, viruses, worms, spyware and logic bomb, ID theft, and miscellaneous (including embezzlement and corruption) are among the top list with most average losses, each of which are beyond one million dollars. The average losses of attack and sabotage, data theft and espionage, and fraud are relatively lower, 160 thousand, 5 thousand and 384 thousand dollars separately.
- Overall, the average loss of the reported 49 cases with is more than 2.989 million dollars. Adding cases without losses reported, the average loss still reaches 1.274 million dollars.

Victims of cybercrime



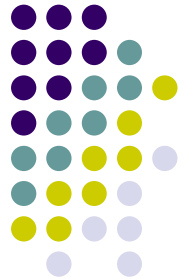
- Private sector is the primary victim of cybercrime. All of the cases of data theft and espionage, ID theft, and fraud are against private interest. Approximately 87.5 percent of miscellaneous (including embezzlement and corruption), approximately 81.8 percent of viruses, worms, spyware and logic bomb, approximately 77.3 percent of attack and sabotage, approximately 69.5 percent of hacking and illegal access are committed against private sector.
- Only approximately 18.2 percent of attack and sabotage, approximately 13.6 percent of hacking and illegal access, and approximately 12.5 percent of miscellaneous (including embezzlement and corruption) are against public sector.
- Besides, approximately 15.3 percent of hacking and illegal access, and approximately 9.1 percent of viruses, worms, spyware and logic bomb cases are against both private and public sectors.
- In addition, approximately 9.1 percent of viruses, worms, spyware and logic bomb, approximately 4.5 percent of attack and sabotage, and approximately 1.7 percent of hacking and illegal access cases are against public health and safety, as it was named.

Guardianship level of the victim



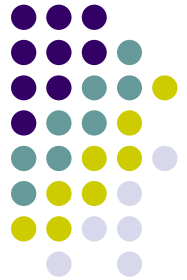
- In majority of cases, the guardianship is weak. Exactly 100 percent of cases of data theft and espionage, and ID theft are possibly due to the absent of related guardianship. In other cases, approximately 90.9 percent of viruses, worms, spyware and logic bomb, approximately 87.5 percent of miscellaneous (including embezzlement and corruption), approximately 82.6 percent of attack and sabotage, approximately 80 percent of fraud, and approximately 74.6 percent of hacking and illegal access are due to weak guardianship.
- Approximately 20 percent of fraud cases, approximately 16.9 percent of hacking and illegal access, and approximately 9.1 percent of viruses, worms, spyware and logic bomb could be classified into the category of medium guardianship.
- Only approximately 17.4 percent of attack and sabotage, approximately 12.5 percent of miscellaneous (including embezzlement and corruption), and approximately 8.5 percent of hacking and illegal access could be stated as with strong guardianship, even though the offences are succeeded.

Complexity of cybercrime



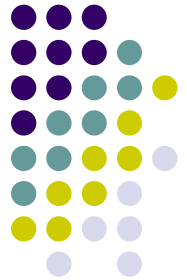
- All the cases of data theft and espionage seem uncomplicated to perpetrate. Approximately 87.5 percent of miscellaneous (including embezzlement and corruption), approximately 80 percent of fraud, approximately 73.9 percent of attack and sabotage, 66.7 percent of ID theft, and approximately 66.1 percent of hacking and illegal access involved no complicated techniques, or techniques that could be available to most common computer or network users at the time of committing such offences.
- Approximately 27.3 percent of viruses, worms, spyware and logic bomb, approximately 20 percent of fraud, approximately 12.3 percent of hacking and illegal access, and approximately 8.7 percent of attack and sabotage cases are committed with a medium level of techniques.
- Cases of viruses, worms, spyware and logic bomb might involve the most complicated techniques, with 72.7 percent of which classified into the most complicated category. Approximately 33.3 percent of ID theft, approximately 18.3 percent of hacking and illegal access, approximately 17.4 percent of attack and sabotage, and approximately 12.5 percent of miscellaneous (embezzlement and corruption) might involve complicated techniques, or techniques unavailable to common users at the time of committing such offences.

Imprisonment sentences



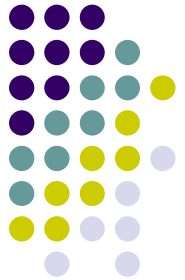
- The punishments for many cases are labeled with “to be decided.” The study calculated the punishment of the sentenced cases. The average imprisonment for the data theft and espionage case is 50 months, the longest among all the categories of cybercrimes. Attack and sabotage, and miscellaneous (embezzlement and corruption) are imposed the same average imprisonment of 40.3 months. Fraudsters obtained an average imprisonment of 32.5 months. Attack and sabotage cases are sentenced with an average imprisonment term of 28.1 months. The shortest average imprisonment term, 21.9 months, is imposed on hacking and illegal access perpetrators, that is, the hackers.
- Total imprisonment term imposed on reported 53 offenders is 1429 months, with an average of shorter than 27 months. Among these cases, the longest imprisonment is 96 months, while the shortest is only one month.

Fine sentences



- Fine is usually imposed on perpetrators of hacking and illegal access, and attack and sabotage. Overall, exactly ten cases ended with fine of lower than 10 thousand dollars, nineteen cases with fine between 10 to 100 thousand, twelve cases with fine between 100 thousand and one million, and two cases with fine over one million dollars (one case fined 2 million and the other case fined 7.8 million dollars).
- The fine imposed on offenders 43 offenders totaled 13.45 million dollars, with an average of 312.78 thousand dollars. However this sum is greatly due to the high fines in two cases where the offenders were fined with 2 and 7.8 millions dollars, which contribute to an average of 228 thousand dollar for each case calculated. Except these two cases, the average fine of the 41 cases is approximately 89 thousand dollars.

Conclusion

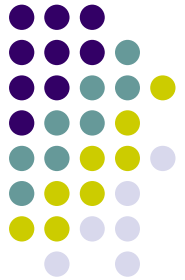


- Easy to commit?
- Difficult to detect?
- Big loss?
- Light punishment?

- More cybercrime…

References

- Becker, J. Who Are the Computer Criminals, *Security Management*, January 1981, pp. 18-20.
- Bequai, August. *Computer Crime*, Lexington, Massachusetts, Toronto: Lexington Books, 1978.
- Howitt, Dennis. *Forensic and Criminal Psychology*, Essex, England: Pearson, 2002.
- Levinson, D. (ed.) *Encyclopedia of Crime and Punishment*, Newbury Park, CA: Sage Publications, 2002.
- Mackenizie, E., and Goldman, K. Computer Abuse, Information Technologies and Judicial Affairs, in *Proceedings of the 28th Annual ACM SIGUCCS Conference on User Services: Building the Future*, 2000, pp. 170-176.
- Meta Group. Security Spending Spree, *PC Magazine*, 20 January 2004.
- Nelson, M. Internet Security Systems' Chris Klaus Says Companies Should Close Back Doors to Be Secure, *InfoWorld,* 10 January 2004.
- Nordic Council of Ministers, *Nordic Information Society Statistics 2005, TemaNord 2005:562*. Copenhagen: Nordic Council of Ministers, 2005.
- Parker, D. B. *Crime by Computer*, Charles Scribner's Sons, New York, 1976.
- Randazzo, Marisa Reddy, Keeney, Michelle, Kowalski, Eileen, Cappelli, Dawn, and Moore, Andrew. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* Carnegie Mellon Software Engineering Institute, August 2004.
- Shannon, L. R. The Happy Hacker, *New York Times*, 21 March 1993, p. 2.
- Shaw, Eric D., Ruby, Keven G., and Post, Jerrold M. The Insider Threat to Information system, *Security Awareness Bulletin*, number 2-98, September 1998.
- Sinrod, E. J., and Reilly, W. P. Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, *Computer and High Technology Law Journal*, volume 16, May 2000, pp. 177-232.
- Syngress. *Scene of the Cybercrime: Computer Forensics Handbook*, Rockland, MA: Syngress Publishing, 2002.
- Underwood, Jim. Criminal Profile, 16 October 2002. Retrieved 8 July 2006, from http://www-staff.it.uts.edu.au/~jim/cit2/cit2-99/legal/CrimProf.html
- Vatis, M. A. *Congressional Statement, Federal Bureau of Investigation, National Infrastructure Protection Center (NIPC) Cyber Threat Assessment, Before the Subcommittee on Technology and Terrorism of the Senate Committee on the Judiciary*, 6 October 1999.
- Ware, H. W., Pfleeger, C. P. and Pfleeger, S. L. *Security in Computing, Englewood Cliffs*, New Jersey: Prentice Hall PTR, 2002.
- Wasik, Martin. *Crime and the Computer*, Oxford: Clarendon Press, 1991.



- Any questions?

Cybercriminology Theoretical Discourses of Cybercrime

Xingan Li, LLD
Faculty of Law
University of Turku

DOI: 10.13140/2.1.4660.0489

Structure

- Lecture: Introduction to theories
- Video: Are Internet Users at Risk?

Primary Criminological Theories

- See “Criminological Theory Summaries”

Theoretical explanations of cybercrime

- Primary references for this lecture:

- Social learning theory
  - Skinner, W. F. and Fream, A. M. A Social Learning Theory Analysis of Computer crime among College Students, Journal of Research in crime and delinquency, Vol. 34, No. 4, 1997, pp. 495-518.
- Routine activity theory
  - Yar, M. The Novelty of 'Cybercrime', European Journal of Criminology, Vol. 4, No. 4, 2005, pp. 407-427.
  - Li, X. Cybercrime and Deterrence, Uniprint, 2008.

Introduction to Social learning theory

- Social learning theory focuses on the learning that occurs within a social context. It considers that people learn from each other, including such concepts as observational learning, imitation, and modeling.

Social Learning Theory

- Social learning theory provides an ideal context in which to understand cybercrime
- 1. It has been empirically verified across numerous studies. It claims to be a general theory that applies to all types of deviant behaviors.
- 2. The very nature of cybercrime requires that individuals learn not only how to operate a highly technical piece of equipment but also specific procedures, programming, and techniques for using the computer illegally.
- 3. An individual learns how to commit crime, and learns specific motives, drives, rationalizations, and attitudes (Sutherland and Cressey 1974, p. 75).

Social Learning Theory

- Social learning theory is organized around four major concepts:
- Differential association
- Differential reinforcement/punishment
- Definitions, and
- Imitation

Social Learning Theory

- Differential association refers to the process by which individuals, operating in different social contexts, become exposed to, and ultimately learn, normative definitions favorable and unfavorable to criminal and legal behaviors (Akers 1994).

Social Learning Theory

- Differential reinforcement/punishment is a concept that captures the diversity of anticipated and actual consequences of engaging in certain behavior. It refers to the balance of social and nonsocial rewards and punishments associated with behavior.

Social Learning Theory

- Definitions are attitudes about certain behavior learned through the process of differential association, imitation, and general interaction or exposure to various sources of learning located in one's social environment. Positive definitions define illegal behavior as desirable, acceptable, and permissible. Negative definitions define illegal behavior as undesirable, unacceptable, and wrong. And neutralizing definitions define illegal behavior as excusable, justifiable, and tolerable.

Social Learning Theory

- Imitation refers to the modeling of certain behavior through the observation of others.

Social Learning Theory

- Test of social learning theory requires operationalizing and measuring numerous variables. Skinner and Fream's article selected only some variables.

Social Learning Theory

- Peer groups are the major social context in which college students interact, and have a great impact on learning cybercrime.
- Face-to-face peer groups
- Virtual peer groups

Social Learning Theory

- Law provides negative definitions of cybercrime: Doing it is wrong, so I don't do it.
- But behaviors and attitudes of peer groups provide positive or neutralized definitions: Others do it, so I do it too.

Social Learning Theory

- Negative relationship between apprehension and software piracy was found by Hollinger (1992). Why?
- Little punishment has been imposed in big cybercrime cases.
- Media sketches how the crime was committed, but not emphasizes how the crime was punished, serving as a course of reinforcement/punishment.
- Certain role models can serve as a source of imitation for cybercrime: family, friends, teachers, and media.

Social Learning Theory

- Multistage sampling procedure:
- 1. Selection of colleges from among 17 within a university that had the highest levels of computer usage by students. Totally 3 colleges were selected: Arts and Sciences, Business and Economics, and Engineering.
- 2. Totally 26 Departments were selected from the 3 colleges: 13 from Arts and Sciences, 5 from Business and Economics, and 8 from Engineering.
- 3. Totally 45 undergraduate classes containing 950 students were randomly selected from those departments. Totally 30 of 45 classes were scheduled to be surveyed, with 581 students.

TABLE 1: Demographics of Sample

Demographics	*Sample*	*University 1992 Enrollment*
Gender		
Female	37.9 (220)	50.4 (12,190)
Male	60.8 (353)	49.6 (12,007)
Race		
White	87.6 (509)	88.1 (21,315)
African American	4.3 (25)	4.1 (998)
Asian	5.9 (34)	1.4 (327)
Other	1.5 (9)	6.4 (1,557)
Age		
18-19	22.4 (130)	19.5 (4,715)
20-21	35.3 (205)	23.0 (5,564)
22-25	29.6 (172)	26.7 (6,463)
26 and over	11.3 (66)	30.6 (7,407)
College		
Agriculture	4.1 (24)	4.5 (1,078)
Arts and Sciences, Natural Sciences	9.5 (55)	6.8 (1,646)
Arts and Sciences, Social Sciences	16.7 (97)	8.0 (1,944)
Arts and Sciences, other	6.4 (37)	17.4 (4,220)
Arts and Sciences, total	32.5 (189)	32.3 (7,810)
Business & Economics	23.1 (143)	11.3 (2,746)
Engineering	29.4 (171)	8.7 (2,107)
Other	10.5 (61)	43.2 (10,456)
Year[a]		
Freshman	10.7 (62)	16.6 (4,027)
Sophomore	19.8 (115)	14.7 (3,550)
Junior	29.3 (170)	15.2 (3,685)
Senior	33.2 (193)	21.5 (5,200)
Graduate	5.0 (29)	20.6 (4,980)
Total	100.0 (581)	100.0 (24,197)

a. High school and fifth-year students were not included.

Social Learning Theory

- Measurement of prevalence and frequency of cybercrime
- 1. Knowingly used, made, or gave to another person a pirated copy of commercially sold computer software.
- 2. Tried to guess another's password to get into his or her computer account or file.
- 3. Accessed another's computer account or files without his or her knowledge or permission just to look at the information or files.
- 4. Added, deleted, changed, or printed any information in another's computer files without the owner' s knowledge or permission
- 5. Wrote or used a program that would destroy someone's computerized data.
- Prevalence rates were calculated as: never, within the past month, within the past year, one to four year ago, and five or more years ago.
- Frequency was calculated as: never, 1 to 2 times, 3 to 5 times, 6 to 9 times, and 10 times or more.

Social Learning Theory

- Differential association was measured using the question: “How many of your best friends have done one or more of the five computer acts?”
- Response: none, just a few, about half, more than half, all or almost all.

Social Learning Theory

- Negative definitions were measured using the question “because it is against the law, I would never do anything illegal using a computer.”
- Response from (1) strongly disagree to (4) strongly agree
- Neutralizing definitions were assessed using 5 statements:
- (1) If people do not want me to get access to their computer or computer systems, they should have better computer security.
- (2) I should be able to look at any computer information that the government, a school, a business, or an individual has on me even if they do not give me access.
- (3) I would never turn in a friend who used, made, or gave to another person a pirated copy of software
- (4) I would never turn in a friend who accessed another’s computer account or files without the owner’s knowledge or permission, and
- (5) It is OK for me to pirate commercial software because it costs too much for me to buy.

Social Learning Theory

- Differential reinforcement/punishment
- Certainty of apprehension
- (1) How likely is it that you would be caught using, making, or giving another person a pirated copy of software?
- (2) How likely is it that you would be caught accessing or trying to access another's computer account or files without his or her knowledge or permission?
- Answers from (1) never to (5) very likely
- Severity of punishment
- (1) How severe do you think the punishment would be if you got caught using, making, or giving another person a pirated copy of software?
- (2) How severe do you think the punishment would be if you got caught accessing or trying to access another's computer account or files without his or her knowledge or permission?
- Answers from (1) not severe at all to (5) very severe

Social Learning Theory

- Imitation was measured using the question "How much have you learned about …from each of the following: (1) family, (2) teachers, (3) books or magazines, (4) television and movies, and (5) computer bulletin boards."
- Answer from (1) learned nothing to (5) learned everything.

Social Learning Theory

- Extent of Cybercrime

TABLE 2: Prevalence of Software Piracy, Guessing Passwords to Gain Unauthorized Access, Unauthorized Access Just to Browse, Unauthorized Access to Change Files, and Writing or Using a Virus by Demographics[a]

	Piracy			*Guessing Passwords*			*Browse*			*Change Files*			*Virus*		
	Lifetime	*Past Year*	*Past Month*	*Lifetime*	*Past Year*	*Past Month*	*Lifetime*	*Past Year*	*Past Month*	*Lifetime*	*Past Year*	*Past Month*	*Lifetime*	*Past Year*	*Past Month*
Gender															
Female (220)	19.5	15.0	3.2	13.6	10.5	3.2	9.5	5.9	1.8	2.3	2.3	0.9	0.0	0.0	0.0
Male (353)	55.5	46.5	18.4	25.2	20.1	6.2	22.7	17.8	4.2	10.5	6.8	2.0	3.4	2.8	0.6
Race															
White (509)	43.4	35.6	13.6	20.6	16.3	4.9	18.5	13.9	5.5	7.8	5.1	1.6	2.2	1.8	0.4
African American (25)	4.0	4.0	0.0	24.0	16.0	4.0	12.0	8.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Asian (34)	38.2	29.4	5.9	14.7	14.7	8.8	8.8	8.8	0.0	8.8	8.8	2.9	2.9	2.9	0.0
Other (9)	33.3	33.3	0.0	22.2	11.1	0.0	11.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Age															
18-19 (130)	33.1	25.4	6.2	23.1	22.3	8.5	16.2	13.8	4.6	5.4	4.6	1.5	1.5	1.5	1.5
20-21 (205)	40.5	36.1	13.2	23.9	18.5	6.3	18.0	13.7	4.9	7.8	4.4	0.5	2.4	2.0	0.0
22-25 (172)	47.1	37.2	16.3	16.3	12.8	1.7	16.3	11.6	3.5	6.4	4.1	1.2	1.7	1.2	0.0
26 and over (66)	47.8	37.3	13.4	16.4	6.0	3.0	22.4	14.9	9.0	11.9	9.0	4.5	1.5	1.5	0.0
College															
Agriculture (24)	45.8	37.5	8.3	33.3	20.8	12.5	20.8	8.3	8.3	12.5	8.3	4.2	4.2	4.2	0.0
Arts and Sciences, Natural Sciences (55)	29.1	21.8	9.1	16.4	20.9	3.6	18.2	12.7	5.5	3.6	3.6	1.8	1.8	1.8	0.0
Arts and Sciences, Social Sciences (97)	43.3	35.1	14.4	20.6	14.4	2.1	18.6	12.4	3.1	7.2	6.2	1.0	3.1	3.1	1.0
Arts and Sciences, other (37)	21.6	18.9	2.7	16.2	16.2	2.7	24.3	24.3	5.4	8.1	5.4	0.0	0.0	0.0	0.0
Business and Economics (134)	32.8	29.1	9.7	20.1	17.2	6.0	14.2	11.2	3.7	6.0	4.5	3.0	0.7	0.7	0.0
Engineering (171)	57.3	47.4	19.9	23.4	18.7	6.4	16.4	12.9	4.7	10.5	5.8	1.2	3.5	2.3	0.6
Other (61)	32.8	23.0	3.3	14.8	13.1	3.3	19.7	13.1	8.2	1.6	0.0	0.0	0.0	0.0	0.0

(continued)

Downloaded from http://jpc.sagepub.com at Turku University Library on December 19, 2008

TABLE 2: Continued

	Piracy			Guessing Passwords			Browse			Change Files			Virus		
	Lifetime	*Past Year*	*Past Month*	*Lifetime*	*Past Year*	*Past Month*	*Lifetime*	*Past Year*	*Past Month*	*Lifetime*	*Past Year*	*Past Month*	*Lifetime*	*Past Year*	*Past Month*
Year															
Freshman (62)	32.3	24.2	8.1	22.6	22.6	4.8	14.5	12.9	3.2	6.5	4.8	1.6	0.0	0.0	0.0
Sophomore (115)	35.7	29.6	7.8	22.6	20.9	10.4	13.9	12.2	7.0	7.8	7.8	1.7	2.6	2.6	1.7
Junior (170)	41.2	35.9	13.5	22.4	15.3	5.3	20.6	14.1	4.1	8.8	4.7	0.6	2.4	2.4	0.0
Senior (193)	43.5	33.7	14.0	18.1	13.0	2.1	19.2	14.0	5.2	6.7	3.6	2.1	2.1	1.0	0.0
Graduate (29)	72.4	65.5	24.1	17.2	13.8	3.4	13.8	10.3	3.4	3.4	3.4	0.0	0.0	0.0	0.0
Total (581)	41.3	33.9	12.4	20.7	16.4	5.0	17.6	13.1	4.8	7.4	5.0	1.5	2.1	1.7	0.3

a. Number of cases in parentheses.

TABLE 3: Frequency and Incidence of Computer Crime in the Past Year

Frequency	*Pirated Software*	*Guessed Passwords*	*Unauthorized Access Just to Browse*	*Unauthorized Access to Change Files*	*Wrote or Used a Virus*
1-2 times	43.9 (87)	73.4 (69)	63.1 (48)	40.0 (10)	85.7 (6)
3-5 times	16.7 (33)	12.8 (12)	13.2 (10)	40.0 (10)	14.3 (< 5)
6-9 times	7.6 (15)	3.2 (< 5)	9.2 (7)	8.0 (< 5)	— —
10 times or more	31.8 (63)	10.6 (10)	14.5 (11)	12.0 (< 5)	— —
Total number of students	100.0 (198)	100.0 (94)	100.0 (76)	100.0 (25)	100.0 (7)
Minimum incidents	906	223	230	82	9
Maximum incidents[a]	1,167+	335+	330+	121+	17+

a. The maximum number of incidents is based on the highest number of each of the given ranges. For the category of "10 times or more," estimates were based on 11 occurrences, so the actual maximum number may be higher.

Downloaded from http://jrc.sagepub.com at Turku University Library on December 19, 2008

Social Learning Theory

- The results of the regression analysis show significant support for the application of social learning theory to illegal computer behavior by college students.

TABLE 4: Standardized (Unstandardized) Regression Coefficients for Social Learning Predictor Variables ($N = 545$)

	Piracy	*Guess Password*	*Illegal Access to Browse*	*Computer Crime Index*
Sources of imitation				
Family	.12 (.18)*	−.06 (−.05)	−.02 (−.01)	.04 (.10)
Teachers	−.05 (−.07)	.05 (.04)	.03 (.02)	.01 (.01)
Books/magazines	.03 (.04)	−.07 (−.05)	.03 (.02)	.02 (.05)
TV/movies	−.07 (−.11)	.01 (.01)	−.07 (−.06)	−.08 (−.20)
Bulletin boards	.04 (.08)	.12 (.13)*	.07 (.08)	.10 (.37)*
Teacher pirated	.12 (.20)*			.14 (.45)*
Teacher encouraged	−.01 (−.03)	.10 (.13)*	−.01 (−.01)	.02 (.09)
Differential association				
Friends	.28 (.38)*	.18 (.13)*	.12 (.09)*	.26 (.62)*
Reinforce-punish				
Certainty-piracy	.03 (.05)			.03 (.10)
Severity-piracy	−.01 (−.02)			.06 (.16)
Certainty-access		.07 (.05)	.02 (.01)	.02 (.04)
Severity-access		−.07 (−.05)	−.13 (−.10)*	−.08 (−.22)*
Definitions				
Against the law	−.15 (−.22)*	−.18 (−.14)*	−.18 (−.15)*	−.23 (−.62)*
Better security		.17 (.13)*	.12 (.09)*	.06 (.15)
Any access		.01 (.01)	.00 (.00)	−.04 (−.09)
Never report friend piracy	.12 (.21)*			.13 (.40)*
Never report friend access		.04 (.04)	.07 (.07)	−.04 (−.11)
Software too costly	.11 (.17)*			.07 (.20)
Control variable				
Gender	−.12 (−.33)*	.01 (.02)	−.04 (−.07)	−.08 (−.39)*
R^2	.37*	.20*	.16*	.40*
M	1.78	1.24	1.23	6.35
SD	1.32	0.68	0.72	2.35

*$p < .05$.

Social Learning Theory

- The sources of imitation operate differently depending on the type of cybercrime: piracy from family and teachers, guessing passwords from teachers, all behavior from computer bulletin boards.
- Differential associating with friends strongly impacts on piracy and computer crime index. Definitions associated with adherence to the laws against these acts are significantly and negatively related to all types of cybercrime.

Social Learning Theory

- Findings:
- Certainty of apprehension was not found negatively related to piracy.
- Severity of punishment for piracy did not predict this type of behavior.
- Certainty of apprehension for illegal access to computer accounts does not deter.
- Severity of punishment was found associated with illegal access.

Social Learning Theory

- Piracy of software was more likely to be neutralized than other acts.

Social Learning Theory

- Female students were significantly less likely to pirate software and be involved in cybercrime than were male students.

Social Learning Theory

- Conclusion:
- Strong support for social learning theory as a conceptual framework for understanding cybercrime in general.

(End of SLT)

Routine Activity Theory

- Routine activity theory is a sub-field of rational choice criminology, developed by Marcus Felson.
- Routine activity theory says that crime is normal and depends on the opportunities available. If a target is not protected enough, and if the reward is worth it, crime will happen. Crime does not need hardened offenders, super-predators, convicted felons or wicked people. Crime just needs an opportunity.
- The basic premise of routine activity theory is that most crimes are petty theft and unreported to the police. Crime is not spectacular nor dramatic. It is mundane and happens all the time.
- Another premise is that crime is relatively unaffected by social causes such as poverty, inequality, unemployment.
- Routine activity theory is controversial among sociologists who believe in the social causes of crime. But several types of crime are very well explained by routine activity theory including copyright infringement, related to peer-to-peer file sharing, employee theft, and corporate crime.

Routine Activity Theory

- Three factors lead to crime:
- Likely offenders
- Suitable targets
- A target can be:
- a person
- an object
- a place
- The absence of capable guardians
- Some examples of capable guardians:
- police patrols
- security guards
- Neighbourhood Watch schemes
- doorstaff
- vigilant staff and co-workers
- friends
- neighbours
- Close Circuit Television (CCTV) systems

Routine Activity Theory

- Crime Triangle (http://www.crimereduction.homeoffice.gov.uk/learningzone/rat.htm)

Routine Activity Theory

- Why cybercriminals are motivated?
- (i) Pursuing information freedom
- (ii) Achieving ego expression
- (iii) Challenging technical difficulties
- (iv) Seeking knowledge
- (v) Testing system security and resilience
- (vi) Adventuring risky online activities
- (vii) Trying programming skills
- (viii) Tentative attacks
- (ix) Expression of hatred
- (x) Hacking for financial gains or avoiding payment

Routine Activity Theory

- (xi) Hacking for educational reasons
- (xii) Changing academic results
- (xiii) Harassment and murder
- (xiv) Launching political movement
- (xv) Launching cyber warfare
- (xvi) Carrying out anti-computer actions
- (xvii) Mimicking cyber Robin Hoods
- (xviii) Practising unfair competition
- (xix) Practising trap marketing
- (xx) Strengthening self-defence

Routine Activity Theory

- (xxi) Hacking for recreation
- (xxii) Employment-related hacking
- (xxiii) Hacking for the hacker community
- (xxiv) Destroying evidence contained in information systems
- (xxv) Sexually motivated misuse of information systems
- (xxvi) Child abuse
- (xxvii) Anti-deviance hacking
- (xxviii) Comprehensive motives
- (xxix) Unclear motive
- (xxx) (Not motivated but) influenced by psychological depression

Routine Activity Theory

- Why cyber targets are exposed?
- The universal accessibility of the Internet
- The invisibility of cyberspace
- The divisibility of digital files
- The low confidentiality of information systems
- Anonymity
- The uncertainty of the future

Routine Activity Theory

- Why guardian is missing in cyberspace?
- The low controllability of the process
- The disputability of content and activities
- The abuse of services
- Lack of law
- Low detection rate
- Weak punishment
- …

Routine Activity Theory

- Conclusion:
- Cyberspace is vulnerable, lacks of protection, and is exposed to potential perpetrators.

(End of RAT)

References

- Akers, Ronald L. 1994. A Social Learning Theory of Crime. Cullen, Francis T. and Robert Agnew. (1999). Criminological Theory: Past to Present. Los Angeles: Roxbury Publishing Company.
- Hollinger, Richard C. 1992. Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access. Security Journal 2 (1): 2-12.
- Li, X. 2008. Cybercrime and Deterrence, Uniprint.
- Skinner, W. F. and Fream, A. M. 1997. A Social Learning Theory Analysis of Computer crime among College Students, Journal of Research in crime and delinquency, Vol. 34, No. 4, 1997, pp. 495-518.
- Sutherland, Edwin H. and Donald R. Cressey. 1974. Criminology. New York: J. B. Lippincott.
- Yar, M. 2005. The Novelty of 'Cybercrime', European Journal of Criminology, Vol. 4, No. 4, 2005, pp. 407-427.

Are Internet Users at Risk?

- Video: Are Internet Users at Risk? By Dr. Thomas Duebendorfer, From http://www.youtube.com

Cybercriminology Countermeasures

Xingan Li, LLD
Faculty of Law
University of Turku

DOI: 10.13140/2.1.4160.3364

Structure

- Tutorials on collective assignment
- Materials: self-study
- Video: US Cybersecurity Policy

The developing of information systems with a higher quality

- The development of a secure system is a preferential choice among all countermeasures. Just as a healthy person can resist diseases, perfect information systems cannot be victimized. However, the perfect system does not exist just as no one is perfectly healthy. In strict scientific terms, it is not possible to demonstrate a cut-off point between security and insecurity. The higher level of security is generally viewed as security, while the lower level of security is generally viewed as insecurity. Most cybercrimes relate to the defects of the systems. Insecure information systems are like defective products or services, for which the producers or providers should be regulated by the law on product-quality control. Secure information systems can be acquired through the establishment of industrial standards and liability for system quality. In the early years of ICT development, there was more focus on usability. With the development of ICT, a standard for higher quality should be adopted to ensure security.

Promoting security awareness

- Cybercrime is merely a serious breach of cybersecurity, which is not ensured because information systems have low controllability as discussed in Chapter 3. Online users should accept suitable education and training to acquire higher security consciousness. Users are direct interest groups in cybersecurity. Social mechanisms relying on cyber police are simply not enough to maintain cybersecurity. Therefore, it is important for users to raise their law-abiding consciousness, grasp technology to prevent abuses, and enhance their ability of self-protection. To a certain extent, the frequent happening of cybercrime results either from lack of a law-abiding conscience or from the lack of a self-protective consciousness. To educate users is an urgent affair, which should be emphasized at the international level, as the WSIS (2003) has proposed:
- "A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade." (Section B5, paragraph 35)
- Some economists may argue that it is prohibitively costly to educate everyone by a specific institution in a specific opportunity at the same time. However, we cannot ignore opportunities for the effective spreading cybersecurity knowledge to any size of audience.

Raising law-abiding consciousness

- Education for the development of a law-abiding conscience follows a tradition of earlier generations, such as Cesare Beccaria. However, law and order in cyberspace has no precedent to follow. It remains disputable as to whether cyberspace constitutes the natural expansion of traditional society. Consequently, it is still arguable whether traditional laws and regulations should be applied to cyber activities, or whether traditional authorities should extend their grasp over a new space. The netizens who migrate to this lawless space behave unconstrainedly. Under cyber sub-culture, hackers defend themselves by their own codes and ethics, refuse to acknowledge the validity of state power, and ignore state jurisdiction over information systems. The assumptions of an anarchic state without regulation or of an autonomic entity with self-regulation are prevalent among technological supremacists. Knowledge and skills make them technical elites on the one hand, ignorance of law and order makes them law-breakers on the other hand. However, in history, talent, knowledge and skills have never become the excuse for crime. Therefore, education is necessary to raise the netizens' law-abiding consciousness in cyberspace just as in society. This law-abiding consciousness falls mostly into the sphere of ethics as well. The "need for ethical management" and "implementing a code" (Bequai 1983, pp. 76-80) has long been recognized. Education in this aspect is a long-term and extensive task for many sectors.

Developing security technology

- Before any scientific discovery and technological invention are made available to the general public, they are controlled in the hands of a few scientists and technicians, regardless of the possible impacts. Nothing about security is preferential. Only when incidents of broad harm to human beings became apparent did the scientific ethics begin to be emphasized in obviously harmful scientific activities. Priority should be given to a swift transition from an emphasis on usable technology to the development of a secure technology. The ICT industry has opportunities of developing security technology and of enhancing users' self-protective ability. Information systems can only be secured through a constantly updated technology, the development of new products, increased self-protection, and the closing of security gaps.

Security training

- Many factors erode the security protection of information systems. Lack of security consciousness and security measures is the most usual reason why users cannot secure their system. Users do not have the incentive to adopt security measures unless their systems are compromised. The usual examples of active participation in security training take place when users suffer losses or when administrative decree forces them to accept training. Users who benefit from security training are willing to receive further training. Nevertheless, in practice, security training is not always effective if it is operated as a market solution, because private trainers have the incentive of gaining pecuniarily from exaggerating risks and dangers, and from the effects of their training. Therefore, the training should better be organized by qualified institutions licensed by the public authorities.

Establishing specific institutions

- Durkheim's ideas concerning the social division of labour argue for specialized organizations in charge of crime prevention. This is because the establishment of institutions specialized in many different fields tends to fall into the hand of a bureaucracy. Social resources are wasted when many new institutions are established while many old institutions are not disestablished. Cybercrime prevention is different. In fact, many countries have established numerous institutions at different levels and on different scales, being affiliated to or independent of other institutions. Independent institutions, equipped with their expertise and knowledge, would be more effective in reacting against urgent incidents. These institutions may take the form of a contact-point such as the 24/ Network designed by the Convention on Cybercrime. The Convention on Cybercrime has provided that each party should authorize a contact-point available on a twenty-four hour, seven-day-a-week base, to guarantee instant support in investigation and collection of evidence. This provision requires member states to bear a round-the-clock responsibility for "immediate assistance."

Reasonably monitoring online activities

- Although there are uncertain factors for maintaining law and order in cyberspace, criminal behaviour should be punished and prevented. The establishment of cyber police and cybercrime reaction forces in many countries meets the demand of security protection. One of the goals of a cyber police and of cybercrime reaction forces is to prevent and monitor harmful online activities, which usually happen within seconds and leaves no trace. The fundamental requirements for cyber police should be profound computing and networking knowledge and anti-hacking skills, as well as the potential to follow new developments of ICT. Because cybercrime can easily cross state borders, rapid reaction and the mutual assistance of cyber police between different countries is vital.

Legislating on cybersecurity

- Consensus has not yet been reached on whether cyberspace should be regulated or deregulated. However, our discussion supports feasible and adequate regulation, without which law and order in cyberspace cannot be maintained. At present, the legal provisions on cybersecurity protection are scattered throughout criminal law, civil law, specific acts, regulations and decisions. It is necessary to implement a law specializing in cybersecurity protection, during which the lessons and experiences of various countries should be drawn upon to strengthen pertinence, systematism, and operability. The improved effectiveness of regulation and an increased severity in punishment would make it more costly to commit cybercrime, and discourage the potential criminals from taking the risk.

Reinforcing judicial effectiveness

- The ICT promotes the effectiveness of all the social activities by making all the participants informed. Cybercrime emerges as a side-product of ICT, which can both strengthen and weaken the effectiveness of the law enforcement based on the traditional social environment. The central problem is that the atmosphere of free cyberspace has an extensive influence. When interception techniques are used in law enforcement, they usually induce disputes from different interest groups. The culture of security should be promoted by the adoption of relevant techniques by the law-enforcement agencies.

Cooperation of the public-private sectors

- Cybersecurity is a relative conception and mixed provision is more efficient. Cybersecurity should be primarily maintained by the private sector, assisted by the public sector, represented by law enforcement. Because of conflict of interests and limited capacity, neither public sector nor private sector can undertake the whole task of cybersecurity protection alone. The absence of public-private cooperation has been one of the critical problems in combating cybercrime (Syngress 2002, p. 2), lack of which just leaves loopholes in cybersecurity unfilled and exposes the vulnerabilities of information systems.
- International society has recognized the importance of cooperation in this field. Three modes of public-private cooperation should be considered: first, public-private partnership; second, public-supported private activities; and third privately-supported public activities. Previously, cooperation was usually organized by the public sector and participated in by the private sector. The authoritative power and administrative function of the public sector played an important role in inducing a broad participation of individuals and enterprises, providing some kinds of education, training, rules, and coordination. The growing interests and forces of the private sector require a strengthened role in providing cybersecurity independently, or interdependently with the public sector.

International cooperation

- **The international highway, railway and airway are limited to territory. The material existence of an information superhighway, however, only appears in sovereignties in the forms of cables and computers. The contents and activities of information systems are intangible, crossing locations distributed possibly anywhere along the "information superhighway." The discussions in the previous chapters have offered abundant revelation that in the current greatly interconnected society, combating cybercrime necessitates global cooperative endeavours, which is required in cybersecurity protection at various levels, including raising international and national levels of security consciousness, harmonizing substantive legislations, filtering and intercepting trans-border information traffic, furthering the exchange of detained judicial information, mutual assistance in criminal investigation, extradition of criminals, and other necessary fields. McConnell International has (2000, p. 8) proposed a "model approach" to cover both international cooperation and private-public partnership to eradicate the legal vacuum. The "common criminal policy" as the Convention on Cybercrime furnishes can be seen as equivalent. A consistent framework of legal policy constitutes the foundation of any international cooperation. In international cooperation, this means the necessary *coordinated* national police actions in search and seizure of stored data, real time collection of traffic data, interception of content data, and so on as provided in the Convention on Cybercrime (Articles 19-21).**

- The present world powers remain intolerant of differences between communities, countries, and cultures. Ours is a world without awaiting and communication before state violence and wars come into being. The failure of broader consensus and broader accommodation of the current international forum reminds the mutual proximity through international, intercultural and interrelated dialogue. The natural logic behind this world is that in a violent world, terrorism has been the excuse of endless wars (against the terrorists) and in information society, cyber terrorism will be the excuse of future wars (against the cyber terrorists). It seems that international cooperation in an equal and a tolerant platform is more than ever required. In the sense of money laundering, developed states, particularly those with a developed banking system, are legally doing far more than a poor country listed as the core of world concern can implicitly or explicitly do. However, international pressure is more than ever put on the poor country rather than its developed counterparts. Therefore, future international cooperation should be carried out in a more balanced way, an approach that should run through all efforts for combating cybercrime.

Reinforcing the deterrence of punishment

- Penal measures are the final remedy for cybersecurity breaches. If criminals are left unpunished, they will have a greater incentive to repeat their activities and gaining even more pecuniary profit from them. Legal history has not witnessed any substitutive measures for punishments, even though the types of punishments change over time. The previous practice proves that deterrence of punishment has been greatly influenced by obstacles to law enforcement. The economic viewpoint on crime and justice argues that low probability of detection and inappropriate severity of punishment would minimize the overall deterrence (Becker 1968). In order to improve the deterrent effect of punishment, both investigation and conviction should be strengthened through a series of techniques and actions. Both national and international legal instruments have been constantly making such efforts. Nevertheless, there are also factors hindering the extreme efforts to reduce the crime-rate simply by increasing investment for improving law enforcement. It would be prohibitively expensive to produce a few effects on crime rate reduction. Therefore, no better alternative is open than that of giving comprehensive consideration to the process of law enforcement in a detailed social context.

Establishing a victim compensation mechanism

- Cybercrime represents a way of transferring information, wealth, competitive power, and psychological satisfaction from victims to perpetrators. Most victims are usually those people with low risk-awareness and a low security level. Furthermore, the victims of cybercrime are generally reluctant to report crimes. They worry that public authorities cannot remedy past damage but can cause further losses by weakening public reputation and inducing future attacks. Victim compensation mechanisms increase the incentives of victims to report crimes and provide evidence, with the help of which they can recover part of losses. Because compensation imposes an extra financial burden on the perpetrators, it also creates incentives to discourage the potential criminals from compromising information systems. Ideally, the dual incentives thus created will decrease the number of cybercrimes.

Eliminating negative incentives in cybersecurity protection

- Cybersecurity involves many different interest groups who benefit from different activities. System developers attempt to reduce costs for improving the security of software. Computer users attempt to reduce their investment on security measures. Security service providers have the incentive to exaggerate the risks, dangers, number and losses of insecurity incidents. The mass media also have the incentive to attract more readers, audience, advertisers, and marketers. Even the police and professors have the possibility of benefiting from increased expenses on research and development. On the other hand, some individuals and institutions have an incentive to underestimate the genuine threat of cybercrime. Countermeasures must be taken to eliminate these incentives that distort truths and exploit these distorted truths of cybersecurity.

Drawing out lessons from traditional crime-prevention practice

- Although cybercrime has many characteristics different from traditional offences, it is a natural development of criminal phenomena, playing an interference opportunities brought about by information systems. The past lessons in failed efforts and experiences in successful endeavours have an organic relationship with current and future-policy design. In fields such as the deterrence of juvenile delinquency, international trafficking of human beings, drug control, and prevention of violence, the existing criminal-justice system proves constructive. The cybercrime scene is less violent, but there are still elements that can be addressed by ordinary methods, such as raising a law-abiding consciousness, by constructing an online community, and by the establishment of an information security culture.

References

- Becker, G. S. 1968. Crime and Punishment: An Economic Approach, Journal of Political Economy, volume 76, pp. 169-217.World Summit on the Information Society (WSIS). 2003. Declaration of Principles. Building the Information Society: A Global Challenge in the New Millennium. Document WSIS-03/GENEVA/DOC/4-E. Geneva, 12 December 2003.
- Bequai, A. 1983. How to Prevent Computer Crime: A Guide for Managers. New York, Chicago, Brisbane, Toronto, Singapore: John Wiley and Sons.
- Li, X. 2008. Cybercrime and Deterrence, Uniprint.
- Syngress. 2002. Scene of the Cybercrime: Computer Forensics Handbook, Rockland, MA: Syngress Publishing.

- Any questions?

Cybercriminology
Social Control in Information Society

Xingan Li, LLD
Faculty of Law
University of Turku

Socia control in cyberspace?

- Max Weber: a formally rational regime
- Thomas Hobbes: *Leviathan* , a “war of all against all”
- Plato: *Republic*
- Thomas More: *Utopia*

Improvement of legal literacy

- Quality of the legal framework and effect of its operation are severely dependent on legal literacy of citizens. Traditionally, legal illiteracy is not even a reason for citizens to be more or less excused, because there is such legal maxim as “ignorantia juris non excusat” (No-one should be excused for ignorance of the law). Here, by legal literacy, we refer to the condition of knowing law by people subjecting them to the order under the constraint of law.

- As far as legal literacy is concerned, the degrees to which literacy exists differ from one to another. There are those who are rather legally illiterate, who are more or less legally literate, and those who are highly legally literate. Certainly, there is hardly one who is absolutely legally illiterate and one who is completely legally literate. Literacy exists on one certain point along the line of degrees between zero percent and one hundred percent.

- Thus far, we can list ideal types of citizens according to different degrees of their legal literacy:
- 1. Those who are illiterate are also legally illiterate of both domestic law and foreign law.
- 2. Those who are literate but are legally illiterate of both domestic law and foreign law.
- 3. Those who are literate are also legally literate of domestic law but not foreign law.
- 4. Those who are literate are also legally literate of foreign law but not domestic law.
- 5. Those who are literate are also legally literate of both domestic law and foreign law.

- The reasons why citizens are illiterate of law are multiple, but two of them are of the most significance: the unawareness of citizens and the unavailability of law.

- The unawareness of law was once a primary factor for citizens to hold an alienate attitude towards any law, be it of civil or criminal nature. In many countries in previous centuries, ties with something “a law” were somewhat bad, unfortunate or mystery. Therefore, persons who were assigned as subjects operating law would be mystified as a result of their priority over power and knowledge, through such symbolic things as crosiers and ritualistic robes; persons who were involved in legal issues would be categorized as either vulnerable individuals who suffered from infringement or invasion from others, or vulgar individuals who imposed infringement or invasion on others. As a whole, law is not a usual practise in daily life and social activities. On the contrary, escaping from law and relevant affairs was preferred by a majority of citizens.

- The awareness of law has been increasingly strengthened over years due to the seriousness and severity of legal issues being decreased and the position of the legal profession being demystified. The current situation is that even though no one knows everything about law, most citizens know something about law. The legal profession is gradually becoming a profession that is increasingly comparable with other specialities, in Durkheim's words, different divisions of labour, in society. Therefore, unawareness of law is gradually becoming a minor reason why citizens are legally illiterate.

- The other important reason why citizens are legally illiterate is the unavailability of law. In ancient times, the universal practise was that “if the penalty remains unknown to all, its power would be immeasurable.” (The words are from the comments by Kong Yingda, a Chinese writer in Tang Dynasty on a classic *Zuozhuan* in the volume of Zhaogong) The function of earlier law was supposedly repressive (See Durkheim 1933). For the ruling class to maintain the repressive ruling order, grasp, control, monopoly, and manoeuvre of the mysteriousness of the legal power is of necessity. With the change of the legal function, the “keeping-unknown” of law became not so important in maintaining the mysterious power of the state. Thus this issue became less significant in unavailability of law. The notion was only one side of the coin of the unavailability of law that kept law far from the reach of citizens. The other side of the coin was that conditions of transportation and communications in the ancient times made it impossible to inform most population of law.

- Thus, the active refusal of law on one hand, and passive refusal of law on the other, severely impeded the widespread of legal bodies, legal knowledge and legal consciousness. The coming of the legal enlightenment did not happen until the end of the Middle Ages.

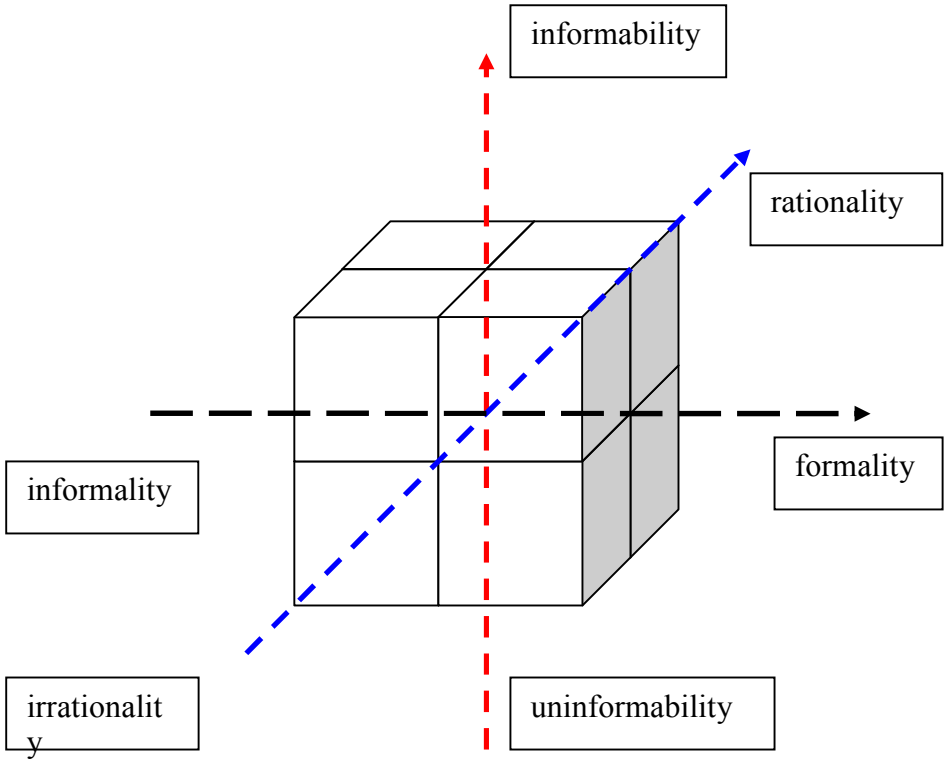
- In modern times, it is not the actual fact that citizens are legally well informed. Even today, states are not fully making efforts to inform their citizens of law. But there is an interfering element in spreading law: the invention of electronic digital computer and the connection of information systems through the publicly-accessible networks. Once the printing technique and wide-distributed libraries made it possible that every citizen could access to available bodies of law. However, it is not a situation where law is available without the limit of time and space. Contemporary information systems change the picture of legal availability and accessibility in providing the possibility of superseding the spatial-temporal boundary of looking up a printed copy.

- Other facilities and inventions did ever improve the availability of law, such as postal system, telephone, telegraphy, and facsimile. But the severe dependence on human resources and the high expenses still left it unreachable to most of the population. Current information systems seemingly apparently overcome the shortcomings of traditional media.
- However, we must bear in mind that doing law (doing medicine, and doing many other scientific practices) is not like doing dictionary looking-up. What we view, read and understand does not equal to what we would receive the reading from specialised legal agencies. Therefore, specialised legal agencies are not substitutable through the common reading of law and widespread of legal knowledge. But it is to satisfy citizens to have a better chance to access to existing law, legal knowledge and achieve higher legal consciousness. All this will help to demystify the legal bodies and the legal profession, and to maintain legal rights and limit the arbitrary power.

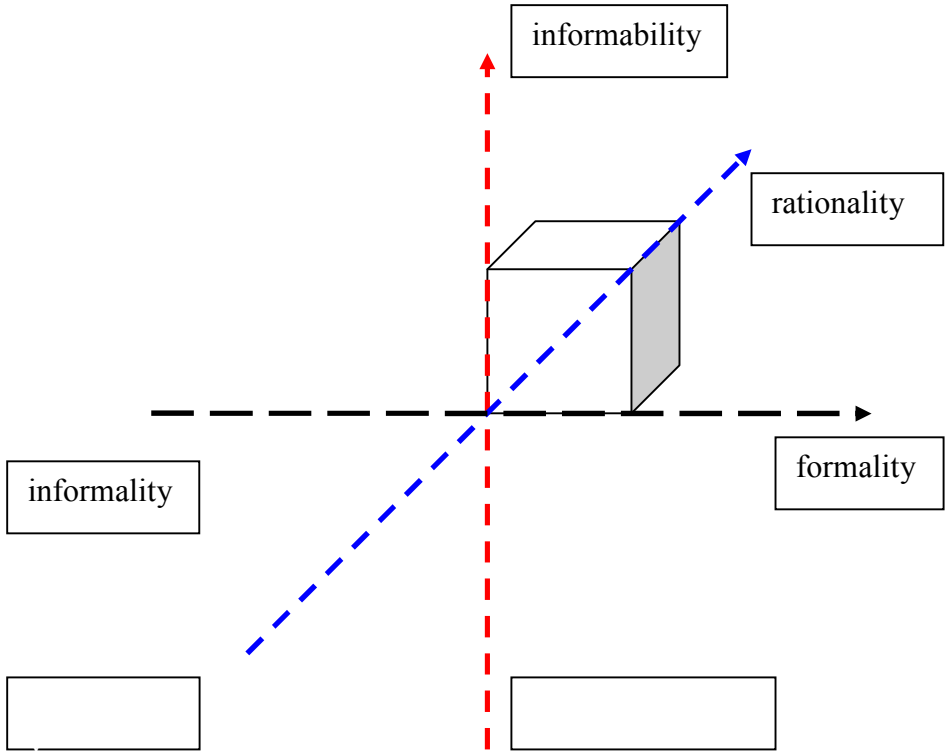
Informed rationality

- When Weber proposed his ideal models of form of law in *Economy and Society*, he had hardly the concern about whether citizens were legally informed or not. Therefore, we could imagine Weber as depicting his models on the premise of citizens being either completely legally informed or completely legally uninformed. But today, we are confronted with increasingly deep concern about the issue whether citizens are legally literate or informed, because we are in an age of being better informable with these tremendous information systems, as we are migratable with the powerful transportation mechanisms.
- If we could suppose the ideal model of form of law in the past was uninformed formal or substantive rationality or irrationality, then our model thereafter should be revised as informed formal (or substantive) rationality (or irrationality). Thus we could put Weber's ideal models into a three-dimensional coordinate system. Borrowing from Weber's four ideal forms of law and legal thought, plus our extra dimension of informability, then we have (The description part of each item mainly refers to the induction of Milovanovic 1994. The part of about informability is my own):

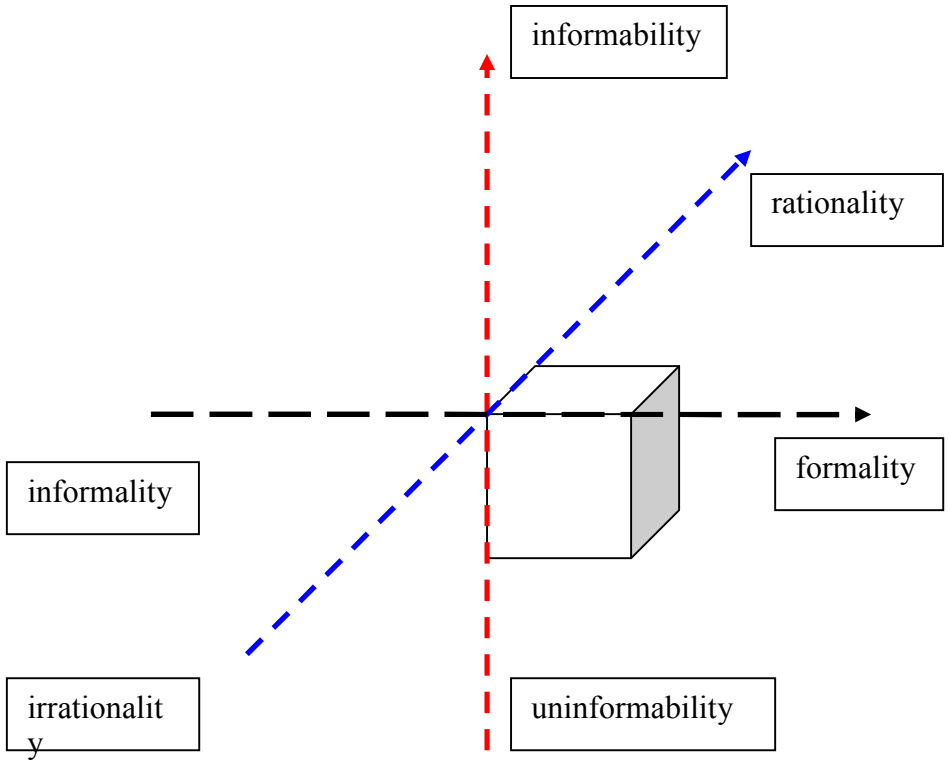
Three-Dimensional coordinate system of forms of law and legal thought



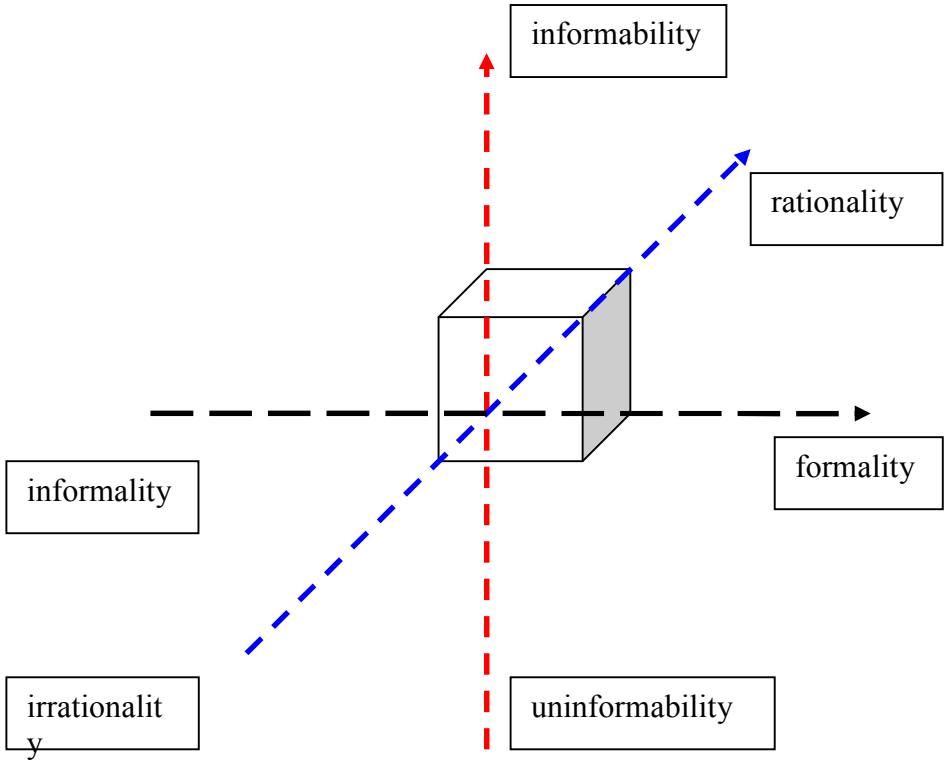
- Informed formal rationality. That is formal rationality with the subjects informed. Under this model, the legal system was operated under the circumstances where clearly-addressed and clearly-observed rules were applied to all like cases in a consistent form. Similarly situated were similarly treated, without external interference with the decision-making process. Besides, the decision-making process has higher degree of transparency by ensuring that the subjects are informed of the applicable rules and/or processes. In sum, this model could be trichotomized as unified criterion, due process, and transparent operation.informalityformalityirrationalityrationalityinformabilityuninformability


informability
rationality
formality
informality

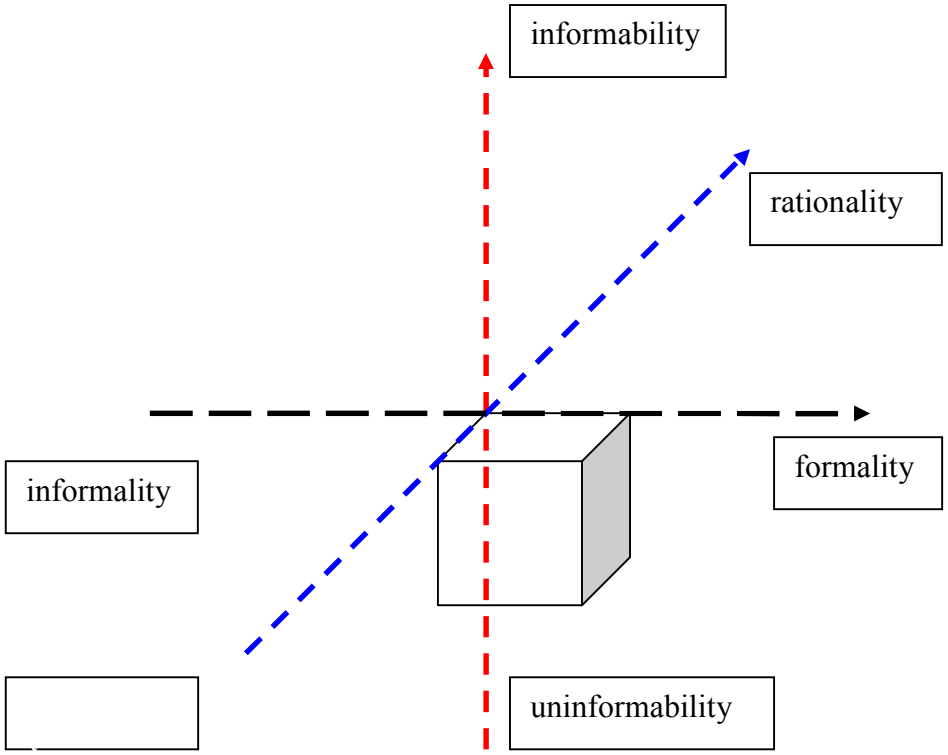
- Uninformed formal rationality. That is formal rationality without the subjects informed. Under this model, the legal system was operated under the circumstances where clearly addressed and observed rules were applied to all like cases in a consistent form. Similarly situated were similarly treated, without external interference with the decision-making process. However, the decision-making process has lower degree of transparency and the subjects are not ensured informed of the applicable rules and/or processes. In sum, this model could be trichotomized as unified criterion, due process, and opaque operation.


informability
rationality
formality
informality
irrationalit
y
uninformability

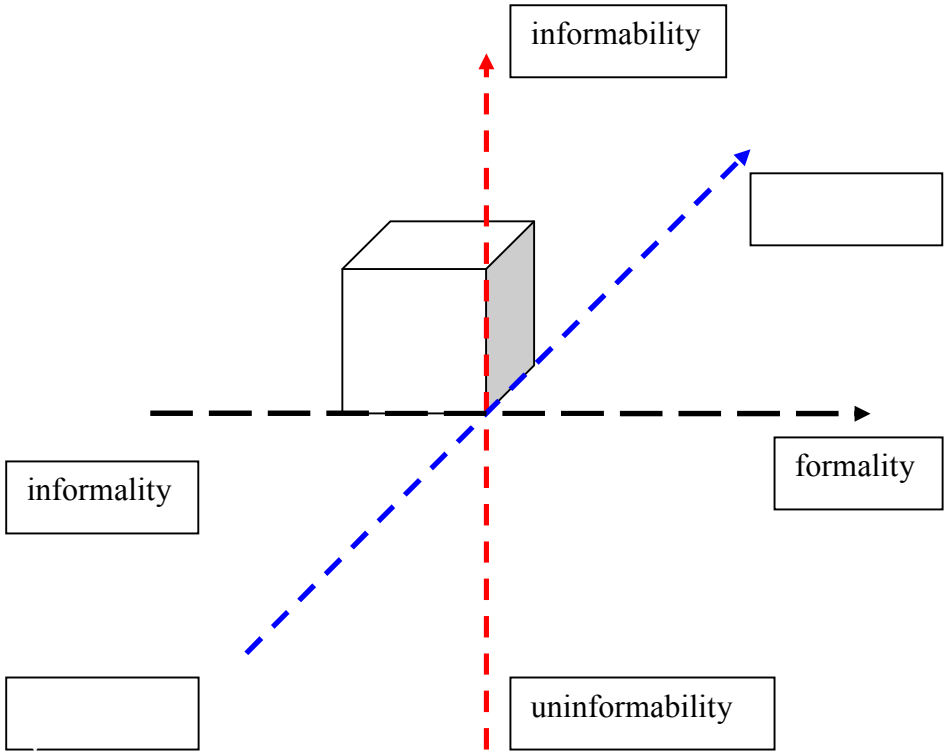
- Informed formal irrationality. That is formal irrationality with the subjects informed. Under this model, the legal system was operated in the process when it is uncertain whether clearly addressed and observed rules were applied to all like cases in a consistent form. Similarly situated were differently treated, with some mysteriously arranged mechanisms functioning in the decision-making process. Arguably, the decision-making process has a certain degree of transparency by providing opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, due process, and transparent operation.


informability
rationality
formality
informality
irrationalit
y
uninformability

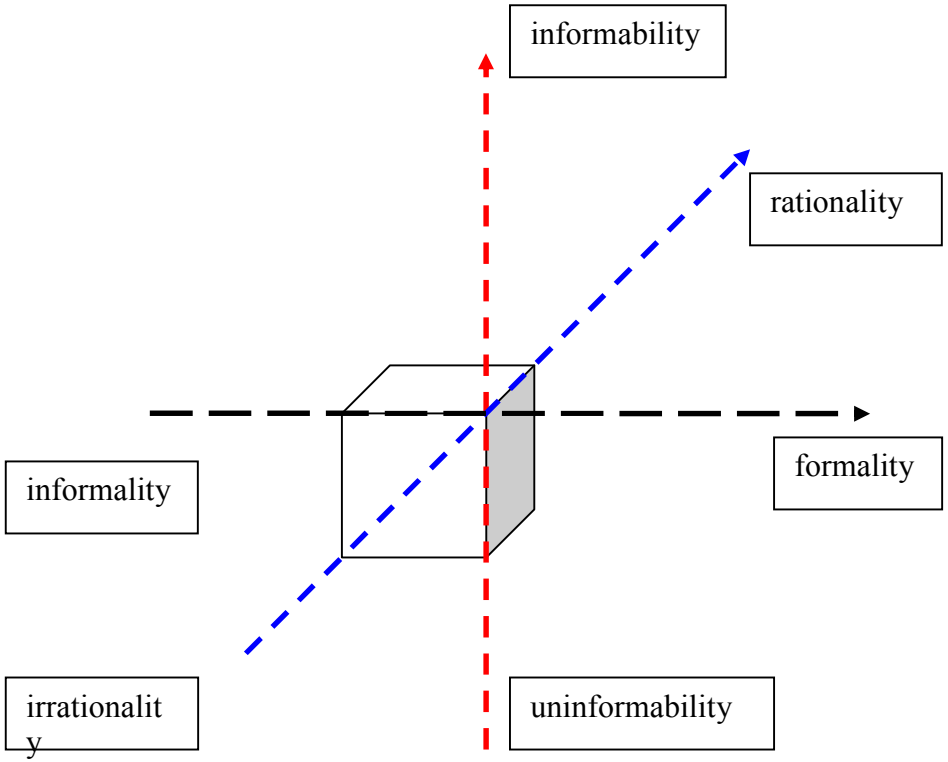
- Uninformed formal irrationality. That is formal irrationality without the subjects informed. Under this model, the legal system was operated in the process when it is uncertain whether clearly addressed and observed rules were applied to all like cases in a consistent form. Similarly situated were differently treated, with some mysteriously arranged mechanisms functioning in the decision-making process. The decision-making process was absolutely secret through depriving any degree of transparency by denying opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, due process, and opaque operation.


informability
rationality
formality
informality
uninformability

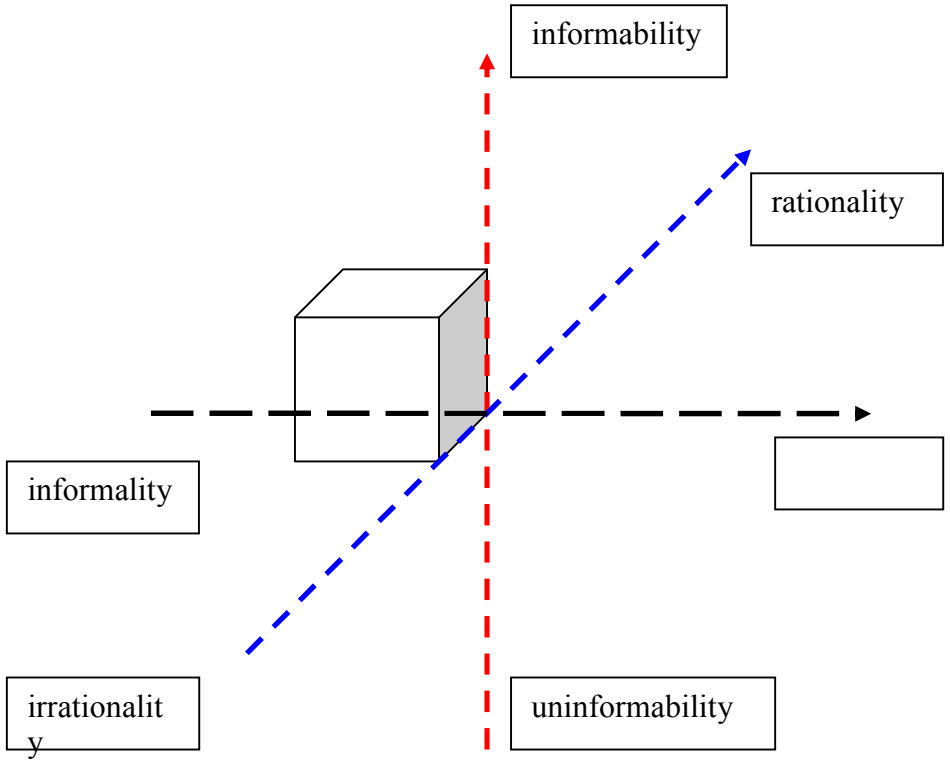
- Informed substantive rationality. That is substantive rationality with the subjects informed. Under this model, the legal system was operated under the circumstances where clearly addressed and observed rules were applied to cases according to the detailed situation. Similarly situated were differently treated, with severe external interference with the decision-making process. Besides, the decision-making process has certain degree of transparency by providing opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and transparent operation.


informability
formality
informality
uninformability

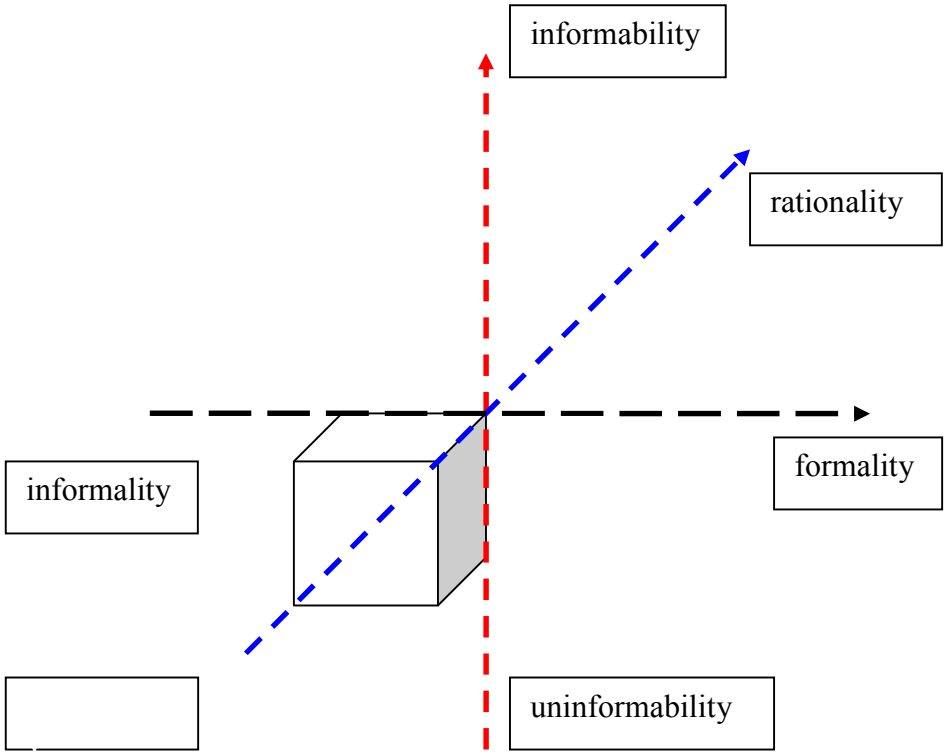
- Uninformed substantive rationality. That is substantive rationality without the subjects informed. Under this model, the legal system was operated under the circumstances where clearly addressed and observed rules were applied to cases according to the detailed situation. Similarly situated were differently treated, with severe external interference with the decision-making process. Furthermore, the decision-making process has no transparency due to denying opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and opaque operation.


informability
rationality
formality
informality
irrationalit
y
uninformability

- Informed substantive irrationality. That is substantive irrationality with the subjects informed. Under this model, the legal system was operated in the process when detailed situation determined the decision. Similarly situated were differently treated, with severe external interference with the decision-making process. Ironically, the decision-making process has certain degree of transparency by providing opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and transparent operation.


informability
rationality
informality
irrationalit
y
uninformability

- Uninformed substantive irrationality. That is substantive irrationality without the subjects informed. Under this model, the legal system was operated in the process when detailed situation determined the decision. Similarly situated were differently treated, with severe external interference with the decision-making process. Furthermore, the decision-making process has no transparency due to denying opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and opaque operation.


informability
rationality
formality
informality
uninformability

- In the past, legal form of law was sunk under the platform of the surface between the informed and the uninformed. That is to say, it was located in a certain point within the part constituted by the points of Uninformability-Informality-Irrationality-Formality-Rationality. Today, it is raised to the level of being informed. Thus we are talking primarily about the informed form of formal (or informal) rationality (or irrationality), located within the part constituted by the points of Informability-Informality-Irrationality-Formality-Rationality. That is the upper part of the coordinate system, which is floating above the surface by information systems.

Primitive Cyber Society

- We could find little evidence on whether the cyber society will repeat or replicate the developmental process of the traditional or non-cyber-society. But we have witnessed a lot of statements that impressed us as if they described the state of the emerging societal existence in relation with information systems as in a primitive stage as that has been had much to be said by writers only in the last several centuries. While whether what they have actually experienced or investigated were “primitive” societies is still to be determined, we could find a publicly recognized model of primitive society characterized by lower developed culture, economy and political structure. The similar happened in the inquiry of the cyber society and an impression of primitive cyber society is quite clear in current literature.

- Hobbes' Leviathan, and Rousseau's state of nature were relatively pessimistic scenarios. Marxian primitive communist society was far more an optimistic picture than theirs. In this primitive communist society, there was no private property, no class and class struggle, no state, no deprivation. People commonly owned productive materials and living materials, commonly worked and lived, and equally distributed products. Only when private property, the source of all evils, emerged did the primitive society become involved into conflicts of interests. Despite all these distinction between the viewpoints on how the primitive society existed, the twentieth century observers from different standpoints viewed the emerging cyber society as different as those who observed the primitive societies several centuries ago.

- Classic writers wrote on the primitive societies from relatively post de facto positions, while the modern writer writes the primitive cyber society from relatively priori de facto positions. It could be safely said that the classical writers hardly ever lived a practical life in the primitive societies they investigated, heard, wrote or imagined. At best they were outside observers of some of the objects, which there were not enough convincing evidences to prove us that they were the just models that preceded societies of our, or more exactly, of the classical writers, they were inquiring. In fact, the practical primitive societies of the current mainstream societies remain unknown to present people. Cyber society, however, has been closely witnessed by many of the commentators who are writing about the developmental process of it. Therefore, the primitive cyber society might be one of the primitive societies that has ever been mostly investigated and written, if there was ever another one that was investigated and written by writers in person.

Internal and external control of cyber society

- Control over a society can be mobilised by either internal or external factors, or in case there is no control at all, by neither internal nor external factors. But it is a rare case where there is no control, or no order at all. However, most writers are claiming that the cyber society is not regulation-free, because order exists everywhere maintained by certain internal or external control mechanisms.
- Society could be regarded as integrity, of which cyberspace is a part. The order of cyberspace is also a part of the integrative order of society. Cyberspace as a social existence, however, has special patterns and could be defined as a sub-societal unit. The order maintenance in cyberspace, therefore, could be achieved by internal control and/or external control (for society as a whole, it is still internal control).

- The internal control is characterized by three considerations: (1) The netizens in the cyberspace could not engage in legislation activities and implement forcibly enacted rules such as constitution or law, but could only compile ethical code with sanctions limited to change and refusal of services; (2) Cyberspace is a place where inheriting inequality prevails and netizens are situated in unequal status due to their inequality before they migrated into the cyberspace; (3) Once established, the internal control has little influence on the external control, but external control has strong impact on internal control. Based on these characteristics, the decision-making process of code of practice for the internal control is hardly run with the principle of democracy and mass participation. Rather, these codes are simply drafted by one or two persons who have more concern with their commercial benefits from the service provision, with a little bit reference to the reaction and comments from the service users. The discretion is at the side of the service providers on the scale.

- The external control is the order maintenance through the external mechanisms outside the cyberspace. The pure external control is where the law and order are solely imposed by the state. There is not such external control with the source of power from any other organs. When we consider the issue of external control, therefore, we are inevitable to put netizens into the web of the real society, which could in no way escape from the constraint of the law and regulation.

- By saying internal and external control, we temporarily separate the cyberspace that does not exist without the connection of information systems, from the meat space, that is, society that has existed without information systems but now integrated information systems into its territory. More safely speaking, the frontier between the cyberspace and society in the broader sense is only drawn for the convenience of this theoretical framework. Otherwise, I am strongly insisting that the cyberspace should more be regarded as the extension and an integral part of society. What are connected by information systems are the elements of this society, but not the elements of this society become independent and connected in a space of their own.

- Absent of internal control, absent of external control
- This is a case where neither internal nor external power was installed to operated deliberate control over the order of the cyberspace. We said it is a rare case with little or no internal or external factor directly controlling over the cyberspace. But there is this kind of argument that claimed to leave the cyberspace maintained by pure technological mechanisms. This is a kind of preset arrangement, with human factors appearing far behind the appearance of their codes and programs.
- Rather than case-by-case judgment over activities in the cyberspace according to existing rules, the order is maintained by preset rules that only deal with variety of situations through mechanical application of unified standard. In sum, this is a kind of technological control, with instant internal or external human elements absent. The model could be depicted as the follow figure:

- Under this model, the cyberspace was in a state of anarchy (anarchy does not necessarily mean confusion). The advocators of anarchic cyberspace claimed that the cyberspace has been created solely by technicians with technology, independent of society, free from the governing of the state, forming a new existing space. This is a kind of space where the human relationships are in the “null-gravity state”. We can well describe it as the balance in the unbalance, the order in the disorder. The activities under such circumstances involve lower cost but take higher risk. Without any regulation and control, the Wild West metaphor of the virtual community will be the most appropriate (Many authors have exploited the metaphor of ”Wild West” about the circumstance of the cyberspace. For random examples, see Morris 1998; Clairmont 1998, pp. E1 and E2).
- Due to the vacuum structure of this kind of cyberspace, the occurrence of collapse and disruption would be a sudden sooner or later. Thereafter, the attempt of internal control, motivated by desire of ownership of interests and dominative power, and/or external control, motivated by maintaining and enlarging existing interests and power, would take place. It is therefore an instable and unacceptable structure.

- Absent of internal control, present of external control
- Under this model, the internal control mechanism is not established. The order maintenance is primarily the task of the extended control from society as a whole. Although society might have different degree of democracy or autocracy, and it would naturally extend the existing mechanisms into the cyberspace, for the cyberspace, an autocracy was created with the absolute and exclusive external control, without a position of internal control, that is, through the participation of the Internet users.
- This autocracy is not an autocracy in its true sense, where a society was controlled by a few people who arbitrarily exercise control over the majority. Here, the cyber autocracy was only under the pressure from outside the cyberspace, lack of any internal control mechanism.
- In addition, autocracy is not one fixed model. Rather than an absolute form of autocracy, the possible forms might differ from each other by the degrees of autocratic nature. At the same time, cyberspace differs from society as a whole in the degree enjoying the control power.

- If netizens enjoy few rights to organize themselves, and the government maintains the order solely, the cyberspace could be subject to higher degree of autocracy, vice versa. The current situation is that the government polices the cyberspace in the way as well as the traditional society. The rate of the cyberpolicemen to the whole population of netizens is close to, or higher than the rate of the policemen to the whole national population. Therefore, the cyberspace might become a special zone of society but not remain syncretised with the social unity.
- Under such a model, the cyberspace is disciplined forcibly by the external power. For society as a whole, the activities would involve higher cost but take lower risk. However, the external control might meet with resistance from the netizens in the organized form. Again, the external control might not completely fulfil the requirements of the running of the cyberspace, which is in a sense like a well built machine. The stepping into the stage of the internal control would be unavoidable.

- Present of internal control, absent of external control
- This mode of cyberspace is organized according to the common ethics established within the online community. While ethics is needed, law is lack. On one hand, it is not possible to implement rules on the level of “law” due to the absence of the legislative power and institution. The available and feasible rules fall on the level of ethical dimension.
- On the other hand, ethical dimension is relatively developed in cyberspace due to the initial independent development and self-regulation practice. The advocators of the mode believe that the ethical mechanism can work well keeping the cyberspace into order. The netizens under this model constraint their own behaviours according to the ethical code of the cyberspace, avoiding from the breach of the cyberspace, and from invading society. However, the internal control might be confronted with the risk of breakdown due to lack of forcible enactment of sanction, and thus induced is the outside interference, that is the filling-in of the external control.

- Present of internal control, present of external control
- By the fourth model, we are seeking to balance between the external control and internal control. Both internal and external control would play roles in the order-maintaining process. This includes a series of balance such as between internal factors, between external factors, and between internal and external factors. The model includes both a certain degree of internal control and a certain degree of external control, in which the activities might involve higher costs but take medium risk.
- The creation of this dual control could either be a result of compromise between the desires of cyberspace as an integral part and as an autonomous zone of society as whole on one hand, and the other parts of society; or be a result of conspiracy between some of the netizens and the other part of society. Regardless of the nature of such compromise or conspiracy, despite the continuous change of balance between powers of internal control and external control, this is the most possible and stable model, be it not within the ideals of many acclamations.
- The leverage in this model could move from the left to the right, that is to say, the degrees of internal control and external control could differ from strong and weak. In some case as depicted in Figure 5 (1), the internal control is weaker but the external control is stronger with the leverage located in the left part deep into the frontier of the internal control. In Figure 5 (2), the internal control and the external control are ideally balanced with the leverage located on the medium frontier between internal control and external control. In Figure 4 (3), the internal control is stronger but the external control is weaker with the leverage located in the right part deep into the frontier of the external control.

- We can hardly draw a conclusion on which model is the beneficial or practical. It is a question of which discourse is the dominant. There are those who advocated the cyber anarchy, leaving the cyberspace as it is, resisting any artificial control either from inside or from outside. Yet their voices have been too weak to be heard by the netizens and non-netizens. Particularly, society's prevalent discourse might not be compatible with an anarchist view. The same is in the cyberspace. Many also argued for solely internal control over the cyberspace, denying the externally imposed state arrangement. However, in this case, it is not words, grammar and reasoning that are functioning. It is the legislature, police, court and jail doing so. Therefore, solely external control rather than solely internal control is more proximate to the goal of the order of the social unity.
- Given neither absolute internal control nor absolute external control is possible, the more acceptable and more stable structure of cyberspace order might be under a mechanism in which the cocktail of internal control and external control is mixed. It is as if the cyberspace is a globe, which the gravity attracts the elements and materials towards the core, while the outside pressure condenses its cubage. As a result, cyberspace exists in a form of a dwarf star, only in which form, cyberspace becomes an integral part of society as a whole, with a stable and acceptable order.

Conclusion

- The change of legal system in the environment where the pervasive use of information systems forms an irresistible force in shaping nearly all lives of society needs specific attention. The discussion above briefly defined the limit of its boundary. While we have the very reason to exclude the so-called virtual space from the current field, we make no attempt to negate the value of further inquiry into the all the unique respects brought about by the development and understanding of the new technologies, which in turn indeed leads the old legal thinking up to a novel platform. It is on this higher level that the hypotheses of improved legal literacy and informed rationality operate. The essay's other objectives are to construct the models of order in cyberspace over which internal and external forces exercise control to varying degrees. Although the information society in general and the cyberspace in particular is designed toward an environment accommodating a more ideal legal system, mechanistic calculable justice standard would not be realizable in an optimistic future.

References

- Bartle, Richard A. 2004. Pitfall of Virtual Property. Retrieved 14 January 2009, from http://www.themis-group.com/uploads/Pitfalls%20of%20virtual%20property.pdf
- Clairmont, Susan. 1998. Police Compare Cyberspace to the Wild West and Dangerous, *The Hamilton Spectator*, 14 August, pp. E1 and E2.
- Dibbell, Julian. 1993. A Rape in Cyberspace, *Village Voice*, Volume 38, Number 51, 12 December. Retrieved 14 January 2009, from http://www.ludd.luth.se/mud/aber/articles/village.voice.html
- Durkheim, Emile. 1933. *The Division of Labour in Society*. Glencoe: The Free Press.
- Fairfield, J. 2005. Virtual Property, Boston University Law review, Volume 85, pp. 1047-1102.
- Hobbes, Thomas. 1962. *Leviathan*, New York: Collier.
- Li, X. 2006. Cyberspace and the Informed Rationality of Law, in Ahti Laitinen, ed. Kirjoituksia oikeussosiologiasta ja kriminologiasta = Writings in the sosiology of law and criminology, Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja.
- Mason, Moya K. (ed.) 1998. Bibliography, in Howard Rheingold, *The Virtual Community*, 2nd Edition. Retrieved 14 January 2009, from http://www.rheingold.com/vc/book/biblio.html
- Milovanovic, Dragan. 1994. *A Primer in the Sociology of Law*, 2nd edition, New York: Harrow and Heston Publishers, pp. 40-47.
- More, Thomas. 1989. *Utopia*, Cambridge: Cambridge University Press.
- Morris, Andrew P. 1998. Feature: The Wild West Meets Cyberspace, *The Freeman: Ideas on Liberty*, Volume 48, Number 7.
- Plato. *The Republic*. Retrieved 14 January 2009, from http://www.gutenberg.org/dirs/etext94/repub13.txt
- *The Twelve Tables*. Retrieved 14 January 2009, from http://www.fordham.edu/HALSALL/ancient/12tables.html
- Weber, Max. 1978. *Economy and Society: An Outline of Interpretive Sociology*, Guenther Roth and Claus Wittich (eds.), Berkeley: University of California Press.
- WSIS Action Line C5: 3rd Meeting, 22-23 May 2008 (Session 3: Cyber-attacks: Are we ready for the battlefield of the 21st Century?), http://www.youtube.com/watch?v=ci9PEZloU_A

Video

- **U.S. CYBERSECURITY POLICY: 2.08 Full Hearing, 1 hours 13 mins**
- http://www.youtube.com/watch?v=PHdCWoP0XOg

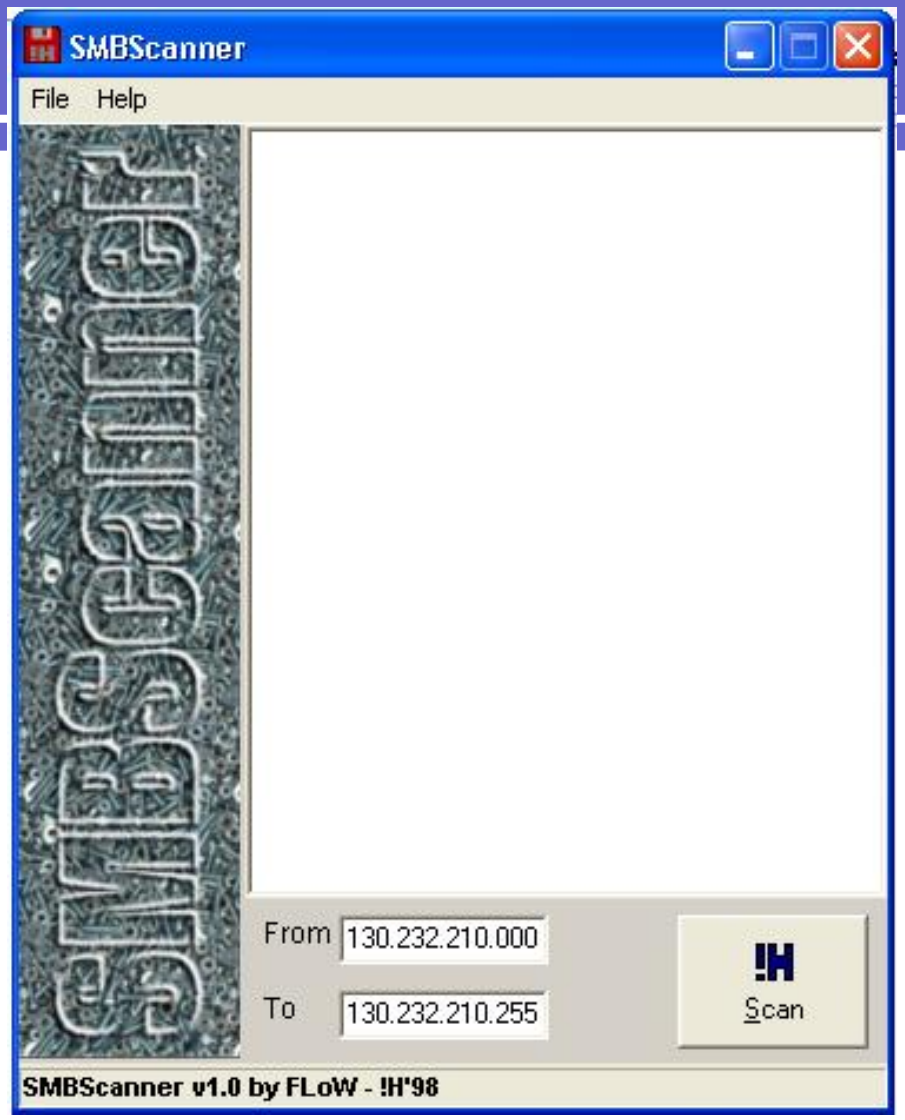
Cybercriminology: Research methods

Xingan Li, LLD
Faculty of Law
University of Turku

DOI: 10.13140/2.1.5184.3367

Experiment

- In scientific inquiry, an experiment is a method of investigating particular types of research questions or solving particular types of problems. The experiment is a cornerstone in the empirical approach to acquiring deeper knowledge about the world and is used in both natural sciences as well as in social sciences.
- An experiment is defined, in science, as a method of investigating less known fields, solving practical problems and proving theoretical assumptions.
- A Simple example: SMBscanner


SMBScanner
File
Help
SMBScanner
From
130.232.210.000
To
130.232.210.255
Scan
SMBScanner v1.0 by FLoW - !H'98

Experience

- Experience as a general concept comprises knowledge of or skill in or observation of some thing or some event gained through involvement in or exposure to that thing or event.
- The concept of experience generally refers to know-how or procedural knowledge, rather than propositional knowledge.
- A person with considerable experience in a certain field can gain a reputation as an expert.

Content analysis

- Content analysis is a methodology in the social sciences for studying the content of communication. Earl Babbie defines it as "the study of recorded human communications, such as books, websites, paintings and laws." It is most commonly used by researchers in the social sciences to analyze recorded transcripts of interviews with participants.
- Content analysis is also considered a scholarly methodology in the humanities by which texts are studied as to authorship, authenticity, of meaning. This latter subject include philology, hermeneutics, and semiotics.
- Harold Lasswell formulated the core questions of content analysis: "Who says what, to whom, why, to what extent and with what effect?." Ole Holsti (1969) offers a broad definition of content analysis as "any technique for making inferences by objectively and systematically identifying specified characteristics of messages." Kimberly A. Neuendorf (2002) offers a six-part definition of content analysis:
- "Content analysis is an indepth analysis using quantitative or qualitative techniques of messages using a scientific method (including attention to objectivity-intersubjectivity, a priori design, reliability, validity, generalizability, replicability, and hypothesis testing) and is not limited as to the types of variables that may be measured or the context in which the messages are created or presented."

Ads by Google

Textalyser

Welcome to the online text analysis tool, the detailed statistics of your text, perfect for translators (quoting), for webmasters (ranking) or for normal users, to know the subject of a text. Now with new features as the anlysis of words groups, finding out the keyword density, analyse the prominence of word or expressions. Webmasters can analyse the links on their pages. More instructions are about to be written, please send us your feedback !

Enter your text to analyze here :

or analyze a website : http://

Analysis options :

- Minimum characters per word : 3
- Special word or expression to analyze :
- Number of words to be analyzed : 10
- Ignore numbers : ☑
- Log the query (only for websites) : ☑
- Apply stoplist : English
- Apply own stoplist (separe with blanks) :
- Make a link analysis : ☐
- Exhaustive polyword phrases : ☐

Analyse the text

Hiden Isochema
Advancing Sorption Analysis
...world leaders in sorption science

all rights reserved 2004 © textalyser.net text analysis V 1.05 help Traduction Hieruchoreici Magazine interactif Umanex Airsoft + Paintball TRANSLATOR HUE LANGUAGE Execution time 0.1848 seconds

Done

ATTENTION SIR/MADAM,

IBTC BANK/UNITED NATIONS SCAM VICTIM COMPENSATION PAYMENT.

This is to bring to your notice that I, Dr. Mrs. Joy Okoy is delegated from the United Nations To Central Bank to pay 150 scam victims $1,000,000.00 (ONE MILLION UNITED STATE DOLLAR) each. You are listed and approved for this payment as one of the scammed victims to be paid this amount, get back to me as soon as possible for the immediate payment of your $1,000,000.00 compensation funds. On this faithful recommendations, we want you to know that during the last U.N. meeting held at Abuja, Nigeria, it was alarmed so much by the world in the meeting on the lose of funds by various individuals to these scams artists operating in syndicates all over the world today.

In other to compensate victims, the U.N Body in conjunction with the Nigerian Government is now paying 150 victims of this operators $1,000,000.00 each in accordance with the U.N. recommendations. Due to the corrupt and inefficient Banking Systems in Nigeria, the payments are to be supervised by the United Nations' Officials and the Central Bank of Nigeria as the corresponding paying bank UNION BANK PLC. According to the number of applicants at hand, 114 Beneficiaries has been paid, half of the victims are from the United States, we still have more 36 left to be paid the compensation of $1,000,000.00 each.

Your particulars was mentioned by one of the Syndicates who was arrested as one of their victims of the operations, you are hereby warned not to communicate or duplicate this message to him for any reason what so ever as the U.S. secret service is already on trace of the other criminals. Other victims who have not been contacted can submit their application as well for scrutiny and possible consideration. You are thereby advised to contact the private client office of the Union Bank Plc in Nigeria or contact, in the person of Sir Philip Nelson with below email address or telephone number.

Name of Officer, Sir Mark Peters
E-mail: sirmarkpeters3@mail.ru
Tel +234 8074690760

You will receive your compensation payment through, DRAFT/ATM PAYMENTS SYSTEM. You will be informed with the modalities as you contact us for details.

Textalyser Results

The complete results, incuding compexity factor, and other features

Total word count :	205
Keyword Density Correct? You Need Links - ask any SEO We're the place to Buy Links! Ads by Google	
Number of different words :	144
Complexity factor (Lexical Density) :	70.2%
Readability (Gunning-Fog Index) : *(6-easy 20-hard)*	8.1
Total number of characters :	2334
Number of characters without spaces :	1331
Average Syllables per Word :	1.7
Sentence count :	30
Average sentence length (words) :	12.63
Max sentence length (words) :	42
(your particulars was mentioned by one of the syndicates who was arrested as one of their victims of the operations you are hereby warned not to communicate or duplicate this message to him for any reason what so ever as the u)	
Min sentence length (words) :	1
(mrs)	
Readability (Alternative) beta : *(100-easy 20-hard, optimal 60-70)*	50.2

Frequency and top words :

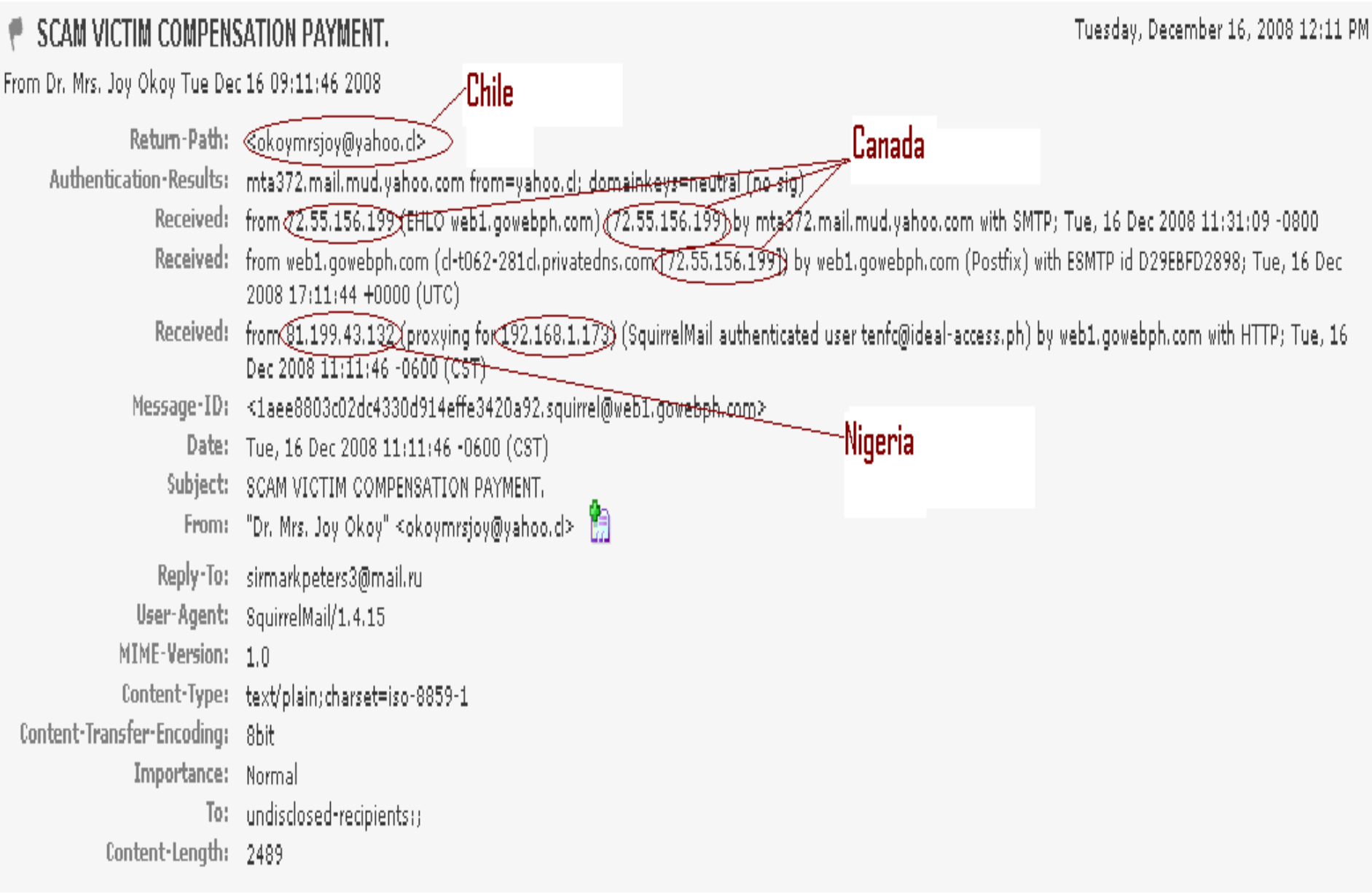
Word	Occurrences	Frequency	Rank
you	7	3.4%	1
victims	7	3.4%	1
united	6	2.9%	2
bank	6	2.9%	2
payment	4	2%	3
nigeria	4	2%	3
compensation	4	2%	3
your	4	2%	3
each	3	1.5%	4
sir	3	1.5%	4

SCAM VICTIM COMPENSATION PAYMENT.

Tuesday, December 16, 2008 12:11 PM

From Dr. Mrs. Joy Okoy Tue Dec 16 09:11:46 2008

Return-Path:	<okoymrsjoy@yahoo.cl>
Authentication-Results:	mta372.mail.mud.yahoo.com from=yahoo.cl; domainkeys=neutral (no sig)
Received:	from 72.55.156.199 (EHLO web1.gowebph.com) (72.55.156.199) by mta372.mail.mud.yahoo.com with SMTP; Tue, 16 Dec 2008 11:31:09 -0800
Received:	from web1.gowebph.com (cl-t062-281cl.privatedns.com [72.55.156.199]) by web1.gowebph.com (Postfix) with ESMTP id D29EBFD2898; Tue, 16 Dec 2008 17:11:44 +0000 (UTC)
Received:	from 81.199.43.132 (proxying for 192.168.1.173) (SquirrelMail authenticated user tenfc@ideal-access.ph) by web1.gowebph.com with HTTP; Tue, 16 Dec 2008 11:11:46 -0600 (CST)
Message-ID:	<1aee8803c02dc4330d914effe3420a92.squirrel@web1.gowebph.com>
Date:	Tue, 16 Dec 2008 11:11:46 -0600 (CST)
Subject:	SCAM VICTIM COMPENSATION PAYMENT.
From:	"Dr. Mrs. Joy Okoy" <okoymrsjoy@yahoo.cl>
Reply-To:	sirmarkpeters3@mail.ru
User-Agent:	SquirrelMail/1.4.15
MIME-Version:	1.0
Content-Type:	text/plain;charset=iso-8859-1
Content-Transfer-Encoding:	8bit
Importance:	Normal
To:	undisclosed-recipients:;
Content-Length:	2489


SCAM VICTIM COMPENSATION PAYMENT.
Tuesday, December 16, 2008 12:11 PM
From Dr. Mrs. Joy Okoy Tue Dec 16 09:11:46 2008
Chile
Canada
Nigeria
Return-Path: <okoymrsjoy@yahoo.cl>
Authentication-Results: mta372.mail.mud.yahoo.com from=yahoo.cl; domainkeys=neutral (no sig)
Received: from 72.55.156.199 (EHLO web1.gowebph.com) (72.55.156.199) by mta372.mail.mud.yahoo.com with SMTP; Tue, 16 Dec 2008 11:31:09 -0800
Received: from web1.gowebph.com (cl-t062-281cl.privatedns.com [72.55.156.199]) by web1.gowebph.com (Postfix) with ESMTP id D29EBFD2898; Tue, 16 Dec 2008 17:11:44 +0000 (UTC)
Received: from 81.199.43.132 (proxying for 192.168.1.173) (SquirrelMail authenticated user tenfc@ideal-access.ph) by web1.gowebph.com with HTTP; Tue, 16 Dec 2008 11:11:46 -0600 (CST)
Message-ID: <1aee8803c02dc4330d914effe3420a92.squirrel@web1.gowebph.com>
Date: Tue, 16 Dec 2008 11:11:46 -0600 (CST)
Subject: SCAM VICTIM COMPENSATION PAYMENT.
From: "Dr. Mrs. Joy Okoy" <okoymrsjoy@yahoo.cl>
Reply-To: sirmarkpeters3@mail.ru
User-Agent: SquirrelMail/1.4.15
MIME-Version: 1.0
Content-Type: text/plain;charset=iso-8859-1
Content-Transfer-Encoding: 8bit
Importance: Normal
To: undisclosed-recipients:;
Content-Length: 2489

Name of Officer, Sir Mark Peters
E-mail: sirmarkpeters3@mail.ru
Tel +234 8074690760

You will receive your compensation payment through, DRAFT/ATM PAYMENTS SYSTEM. You will be informed with the modalities as you contact us for details.

Name of Officer, Sir Mark Peters
E-mail: sirmarkpeters3@mail.ru
Tel +234 8074690760

You will receive your compensation payment through, DRAFT/ATM PAYMENTS SYSTEM. You will be informed with the modalities as you contact us for details.

Case study

- Case study methods involve an in-depth, longitudinal examination of a single instance or event: a case. They provide a systematic way of looking at events, collecting data, analyzing information, and reporting the results. As a result the researcher may gain a sharpened understanding of why the instance happened as it did, and what might become important to look at more extensively in future research. Case studies lend themselves to both generating and testing hypotheses.
- Example: WinCapita, search with Google search engine

Search results of the case of WinCapita in Google

- · ***WinCapita* - Wikipedia, the free encyclopedia**
- *WinCapita*, previously WinClub, was an Internet-based investment club, advertising that it was engaged in currency trading. It operated on the Finnish market **...**
  *en.wikipedia.org/wiki/**WinCapita** - 26k* - Cached - Similar pages
- · ***WinCapita* ponzi scam warning - Faktat**
- *Wincapita* says that it is global company: english pages are showed as a proof of that. The language used on those pages are even worse than this translation **...**
  ***wincapita**-ponzi-warning.weebly.com/faktat.html - 17k* - Cached - Similar pages
- · ***Wincapita* at Nobullshit Network Forum**
- 10 posts - Last post: 6 Mar
- Hi, Has anyone here heard of the organisation which I believe started in Finland and has been operating for 4 years, but is FX for the last **...**
  *nobsnetwork.net/forex-discussions/2655-**wincapita**.html - 96k* - Cached - Similar pages
- · ***Wincapita* on Page 2 at Nobullshit Network Forum**
- 10 posts - Last post: 19 Mar
- *WinCapita* ponzi scam warning - Faktat has some warning signs about **...** Actually they are tried to bring down winclub/*wincapita* over 2 years. **...**
  *nobsnetwork.net/forex-discussions/2655-**wincapita**-2.html - 97k* - Cached - Similar pages
  More results from nobsnetwork.net »
- · **Video results for *wincapita***
- YouTube - *WinCapita* / WinClub puhallus
  2 min 51 sec
  *www.youtube.com*YouTube - *wincapita* stand-up 100% nauruvipu
  2 min 36 sec
  www.youtube.com· ***WinCapita* Suspect Found in Sweden | News | YLE Uutiset | yle.fi**
- The main suspect in the *WinCapita* investment scheme Hannu Kailajärvi has been taken into custody in Sweden. Finland has requested his extradition. **...**
  *yle.fi/uutiset/news/2008/12/**wincapita**_suspect_found_in_sweden_425585.html - 32k* - Cached - Similar pages

More…

- · ***WinCapita* investigation**
- 25 Mar 2008 **...** At the initial stage of the pre-trial investigation concerning the investment club *WinCapita* (former WinClub), the police focus on the money **...**
  www.poliisi.fi/poliisi/krp/home.nsf/pages/87736A1CB0948C3DC225742900541B5F - 9k - Cached - Similar pages
- · **Helsingin Sanomat - International Edition - Home**
- Police looking for main suspect in *WinCapita* fraud case **...** The Tampere native is suspected of having run the *WinCapita* investment club, which collected **...**
  *www.hs.fi/english/article/Police+looking+for+main+suspect+in+**WinCapita**+fraud+case/1135241093766* - Similar pages
- · **Helsingin Sanomat - International Edition - Home**
- *WinCapita* fugitive arrested in Swedish town Hannu Kailajärvi **...** Kailajärvi is not the only fugitive wanted in the *WinCapita* case. **...**
  *www.hs.fi/english/article/**WinCapita**+fugitive+arrested+in+Swedish+town/1135242074800* - Similar pages
  More results from www.hs.fi »
- · **Aapotsikko: Ponzi file #734529: *Wincapita***
- 19 Mar 2008 **...** I sincerely hope that the recent *Wincapita* (of which there's some excellent commentary in Finnish here, and a little bit information in **...**
  *aapocalypsenow.blogspot.com/2008/03/ponzi-file-734529-**wincapita**.html - 87k* - Cached - Similar pages
- · ***wincapita*.com**
- www.*wincapita*.com, https3a2f2fwww.*wincapita*.com, https3a5c5cwww.*wincapita*.com and comhttps3a2f2fwww.*wincapita*.com are subdomains to this hostname. **...**
  *www.robtex.com/dns/**wincapita**.com.html - 29k* - Cached - Similar pages
- · ***wincapita*.net**
- dns information about *wincapita*.net. **...** *wincapita*.net is a domain controlled by two nameservers at domaincontrol.com. They are on different IP networks. **...**
  *www.robtex.com/dns/**wincapita**.net.html - 42k* - Cached - Similar pages
  More results from www.robtex.com »
- · **Aamulehti.fi | Teemat**
- - [Translate this page]
- Hän on myös ilmoittanut *WinCapita*-tulonsa valuuttakauppojen tuottoina verottajalle. Poliisi ei ole kuitenkaan vielä kuulustellut häntä. **...**
  *www.aamulehti.fi/teema/**wincapita**/ - 20k* - Cached - Similar pages
- · **: -) *W I N C A P I T A* -videot - Suomi24 Keskustelu**
- Näytä aiheet. : -) *W I N C A P I T A* -videot. Kirjoittanut: crap;heine 8.4. 2008 klo 00.26. http://www.grapheine.com/bombaytv/play_uk.php?id=186493 6 **...**
  keskustelu.suomi24.fi/show.fcgi?category=500000000000003&conference=4500000000000561&posting... - 43k - Cached - Similar pages
- · ***Wincapita* - sfnet.harrastus.visailu | Google Groups**
- From: Henrik Lahti <la...@liettua.com>. Date: Sun, 18 May 2008 18:51:58 +0000 (UTC). Local: Sun, May 18 2008 2:51 pm. Subject: Re: *Wincapita* **...**
  groups.google.com/group/sfnet.harrastus.visailu/browse_thread/thread/b1e444af0520de35/0a838bef32c6cbab?lnk=raot - 37k - Cached - Similar pages
- · **Finnish police say no currency deals by *WinCapita***
- According to the police, *WinCapita* promised tens of thousands of **...** The NBI added that about 800 people had reported *WinCapita* to the police after losing **...**
  *www.helsinkitimes.fi/htimes/index.php?option=com_content&view=article&id=3084:finnish-police-say...**wincapita**... - 35k* - Cached - Similar pages
- · ***wincapita*.com - Traffic Details from Alexa**
- Alexa Traffic Graphs for *wincapita*.com - Alexa computes traffic rankings by analyzing the Web usage of millions of Alexa Toolbar users.
  *www.alexa.com/data/details/traffic_details/**wincapita**.com - 28k* - Cached - Similar pages
- · ***Wincapita*.com - *WinCapita***
- *Wincapita* has been a customer at root eSolutions for a few months (product: www. server.lu) until they stopped paying their monthly bills a few months ago. **...**
  *whois.domaintools.com/**wincapita**.com* - Similar pages
- · **NewsRoom Finland**
- 12 Dec 2008 **...** He is suspected of leading *WinCapita*, an internet scam. **...** Chief *WinCapita* suspect arrested in Sweden 12.12.2008 **...**
  virtual.finland.fi/stt/showarticle.asp?intNWSAID=20548&group=General - 7k - Cached - Similar pages

- More reliable case study: decided cases
- Example: FindLaw Cases and Codes, http://www.findlaw.com/casecode/

Content of cases

- **Opinion**
- **Facts**
- **Discussion**
- **Sentence**

- **USA v. Sablan--FACTS**
- In the early hours of August 15, 1992, Sablan, a former employee of the Bank of Hawaii's Agana, Guam branch, left a bar where she had been drinking with a friend. Sablan had recently been fired from the bank for circumventing security procedures in retrieving files. That morning, Sablan left the bar and entered the closed bank through an unlocked loading dock door. She went to her former work site (using a key she had kept) and used an old password to log into the bank's mainframe. Sablan contends that she then called up several computer files and logged off. The Government asserts that Sablan changed several of the files and deleted others. Under either version, Sablan's conduct severely damaged several bank files. Sablan was charged with computer fraud in violation of 18 U.S.C. S 1030(a)(5) (the "computer fraud statute"). In a pretrial motion to dismiss, Sablan attacked the statute for its failure to require a mens rea for each of the essential elements of the offense. In the alternative, Sablan requested a jury instruction that required the Government to prove intent as to all elements of the crime. In particular, Sablan wanted the jury to be instructed that the Government needed to prove that she had the intent to damage bank files. The district court denied the motion and ruled that, as used in the computer fraud statute, the word "intentionally" applied only to the access element of the crime. Sablan then entered into a conditional plea agreement that preserved her right to appellate review of the issue raised in her motion.
- The district court calculated Sablan's sentence under Sentencing Guideline S 2F1.1(a), and enhanced her sentence due to the amount of damage caused by Sablan's conduct. The calculation included the cost of numerous hours of computer programming to restore the damaged files. Sablan asserts that the district court improperly calculated the amount of damage due to her actions and that the improper calculation led to (1) an improperly enhanced sentence, (2) a refusal to depart downward, and (3) an improper restitution order.

Interview

- An interview is a conversation between two or more people (the interviewer and the interviewee) where questions are asked by the interviewer to obtain information from the interviewee.
- Example: Online interview

Participant observation

- Participant observation is a set of research strategies which aim to gain a close and intimate familiarity with a given group of individuals (such as a religious, occupational, or subcultural group, or a particular community) and their practices through an intensive involvement with people in their natural environment, often though not always over an extended period of time.

- Example: Second Life, My Space, and so on

Questionnaire

- A questionnaire is a research instrument consisting of a series of questions and other prompts for the purpose of gathering information from respondents. Although they are often designed for statistical analysis of the responses, this is not always the case.
- Questionnaires have advantages over some other types of surveys in that they are cheap, do not require as much effort from the questioner as verbal or telephone surveys, and often have standardized answers that make it simple to compile data. However, such standardized answers may frustrate users. Questionnaires are also sharply limited by the fact that respondents must be able to read the questions and respond to them. Thus, for some demographic groups conducting a survey by questionnaire may not be practical.
- As a type of survey, questionnaires also have many of the same problems relating to question construction and wording that exist in other types of opinion polls.

Statistical analysis

- Statistics is a mathematical science pertaining to the collection, analysis, interpretation or explanation, and presentation of data. It also provides tools for prediction and forecasting based on data. It is applicable to a wide variety of academic disciplines, from the natural and social sciences to the humanities, government and business.
- Statistical methods can be used to summarize or describe a collection of data; this is called descriptive statistics. In addition, patterns in the data may be modeled in a way that accounts for randomness and uncertainty in the observations, and are then used to draw inferences about the process or population being studied; this is called inferential statistics. Descriptive, predictive, and inferential statistics comprise applied statistics.
- Example 1. Australian Institute of Criminology, http://www.aic.gov.au/stats/crime/cybercrime.html
- Example 2. Li, X. Hallmarks of Cybercrime, UOLTJ article

Crime and criminal justice statistics

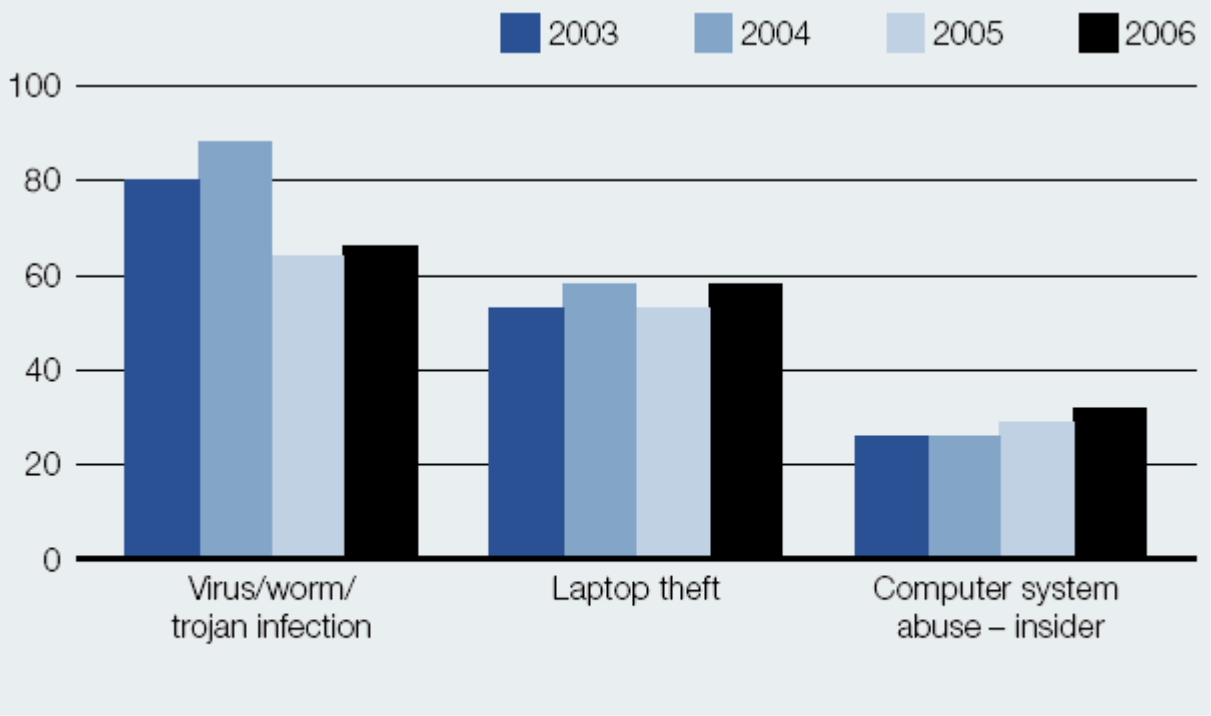
Cybercrime

As few police agencies identify cybercrimes separately, the chart below presents results of the Australian High Tech Crime Centre and various state, territory and federal police agencies. On technology, federal and state government, utilities, finance, and education sectors responded

These data are indicative only as the sample is not necessarily representative. Caution therefo

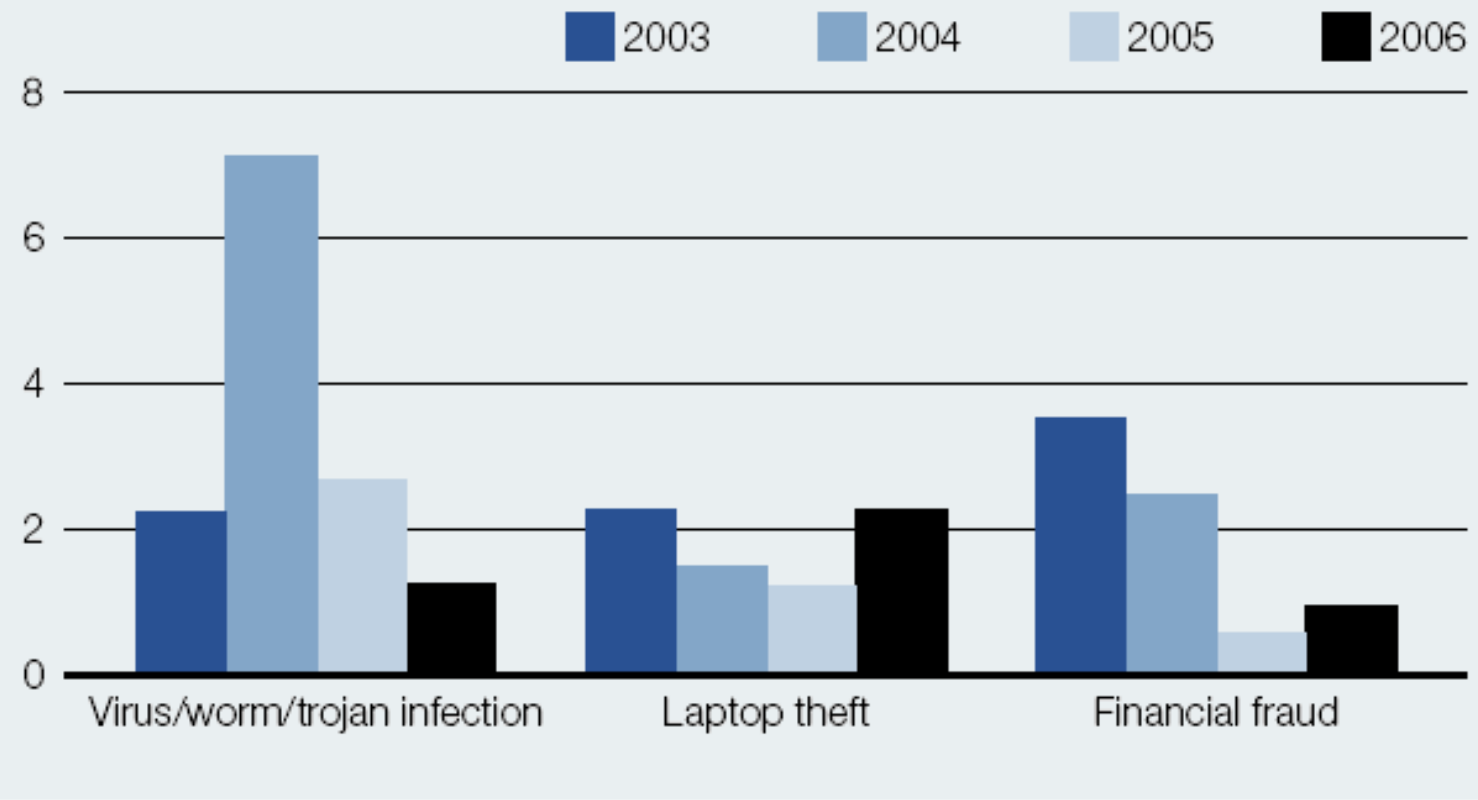
Differences published in previous editions of Facts & figures may be due to differences in the these organisations reported experiencing electronic attacks that harmed the confidentiality, i *facts and figures 2005*)

Most common computer crime and security breaches, 2003-06 (percent)



Source: Australian Institute of Criminology 2007. *Australian crime : facts and figures 2006*. Canberra: AIC

Major sources of financial loss due to computer crime and security breaches, 2003-06 ($ million)



Source: Australian Institute of Criminology 2007. *Australian crime : facts and figures 2006*. Canberra: AIC

Example 2

		Hacking, illegal access		Attack, sabotage, botnet		Virus, worms, spyware, logic bomb		Data theft, espionage		ID theft		Fraud		Other: embezzling, corruption	
		No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Gender	Male	61	96.8	23	100	11	100	7	100	26	100	7	100	13	92.9
	Female	2	3.2	0	0	0	0	0	0	0	0	0	0	1	7.1
	Total	63	100	23	100	11	100	7	100	26	100	7	100	14	100
Age	-16	2	3.2	0	0	1	0	0	0	0	0	0	0	0	0
	17-25	20	31.7	7	30.4	2	18.2	0	0	5	19.2	3	42.9	4	28.6
	26-35	18	28.6	6	26.1	2	18.2	3	42.9	1	3.8	2	28.6	7	50
	36-45	12	19	2	8.7	3	27.3	1	14.3	0	0	2	28.6	1	7.1
	46-	1	1.6	1	4	1	9.1	2	28.6	1	3.8	0	0	0	0
	N/A	10	15.9	7	30.4	2	18.2	1	14.3	19	73.1	0	0	2	14.3
Perpetrator	Insider	15	23.8	3	13	2	18.2	7	100		0	4	57.1	1	7.1
	Outsider	48	76.2	20	87	9	81.8	0	0	26	100	3	42.9	13	92.9
	Former employee	Inclu. 8	12.7	Inclu. 10	43.5	0	0	0	0	0	0	0	0	1	7.2
Loss	No	33	N/A	12	N/A	7	N/A	5	N/A	1	N/A	4	N/A	6	N/A
	-10k	4(21k)	N/A	2(10k)	N/A	1(5k)	N/A	1(5k)	N/A	0	N/A	0	N/A	0	N/A
	10k-100k	15(753k)	N/A	3(69k)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	100k-1m	4(1076k)	N/A	6(1,679M)	N/A	0	N/A	0	N/A	0	N/A	1(384k)	N/A	1(875k)	N/A
	1m-	5(34.3M)	N/A	0	N/A	3(93M)	N/A	0	N/A	2(8M)	N/A	0	N/A	1(6.3M)	N/A

	Total	28(36.15M)	N/A	11(1,758M)	N/A	4(93.005M)	N/A	1(5k)	N/A	2(8M)	N/A	1(384k)	N/A	2(7.175k)	N/A
Citizenship	Foreigner	1 case	N/A	1case	N/A	0	N/A	0	N/A	1case	N/A	1case	N/A	1case	N/A
Imprisonment	1-6	5(24)	N/A	2(11)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	7-12	9(101)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	13-24	7(136)	N/A	4(81)	N/A	2(80)	N/A	1(18)	N/A	0	N/A	0	N/A	0	N/A
	25-36	7(224)	N/A	2(72)	N/A	0	N/A	1(36)	N/A	0	N/A	2(65)	N/A	2(70)	N/A
	37-	4(217)	N/A	2(117)	N/A	1(41)	N/A	1(96)	N/A	0	N/A	0	N/A	1(51)	N/A
	TBD	27	N/A	13	N/A	5	N/A	3	N/A	3	N/A	3	N/A	5	N/A
Fine	-10k	7(31.6k)	N/A	1(5k)	N/A	1(5k)	N/A	0	N/A	0	N/A	0	N/A	1(5k)	N/A
	10-100k	13(512.6k)	N/A	5(187.8k)	N/A	1(17k)	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	100k-1m	5(1.368M)	N/A	4(643.80k)	N/A		N/A	0	N/A	0	N/A	2(624k)	N/A	1(250k)	N/A
	1m-	0	N/A	0	N/A	1(2m)	N/A	0	N/A	0	N/A	0	N/A	1(7.8M)	N/A
	TBD	32	N/A	13	N/A	7	N/A	6	N/A	3	N/A	3	N/A	5	N/A
Nature of victim	Public	8	13.6	4	18.2	0	0	0	0	0	0	0	0	1	12.5
	Private	41	69.5	17	77.3	9	81.8	5	100	3	100	4	100	7	87.5

	Private, public	9	15.3	0	0	1	9.1	0	0	0	0	0	0	0	0
	Public health and safety	1	1.7	1	4.5	1	9.1	0	0	0	0	0	0	0	0
	N/A														
Guardianship on the side of victim	Strong	5	8.5	4	17.4	0	0	0	0	0	0	0	0	1	12.5
	Medium	10	16.9	0	0	1	9.1	0	0	0	0	1	20	0	0
	Weak	44	74.6	19	82.6	10	90.9	6	100	3	100	4	80	7	87.5
Technique availability to others	Complicated	11	18.6	4	17.4	8	72.7	0	0	1	33.3	0	0	1	12.5
	Medium	9	12.3	2	8.7	3	27.3	0	0	0	0	1	20	0	0
	Simple	39	66.1	17	73.9	0	0	6	100	2	66.7	4	80	7	87.5

4. Insider versus outsider

Insiders and outsiders constitute different ratios in different categories of offences. The categories in which the insiders constitute the majority of offenders include: offenders of data theft and espionage were insiders, while 57.1 percent of fraudsters are insiders.

The categories in which outsiders constitute the majority of offenders include: exactly 100 percent of ID theft, approximately 92.9 percent of miscellaneous (including embezzlement and corruption), approximately 87 percent of attack and sabotage, approximately 81.8 percent of viruses, worms, spyware and logic bomb, and approximately 76.2 percent of hacking and sabotage. In fact, outsiders also constitute a strong ratio in fraudsters: approximately 42.9 percent.

The former employees are included in the category of outsiders. A significant ratio of offenders of attack and sabotage are former employees, who constitute approximately 43.5 percent. Former employees also constitute 12.7 percent of offenders of hacking and illegal access, and approximately 7.2 percent of offenders of embezzlement and corruption.

Overall, insiders and outsiders constitute 21 percent and 79 percent of all reported offenders separately. The former employees constitute 16 percent of all of the outsiders. If add up former employees into insiders, they would constitute about 34 percent of the total offenders, still a less ratio than outsiders.

The Criminal Phenomenon on the Internet:
Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted

Xingan Li, Faculty of Law, University of Turku, Finland

ABSTRACT

With the deepening of the research on cybercrime, the hallmarks of cybercriminals and the guardianship of cybervictims are paid increasing attention by lawyers and law enforcement. The purpose of this study is to present an updated profile of cybercriminality and cybervictimization based on practical materials. The study used a sample of 115 typical cases prosecuted (during 18 March 1998 to 12 May 2006), published officially on the web site of the United States Department of Justice. The study found that males are responsible for a majority of these cybercrimes. The cybercriminals distribute primarily among the ages between 17 to 45 years old. Domestic perpetrators constitute the absolute majority of the cybercriminals. Outsiders are four times more likely to be involved in cybercrimes than insiders. Most cybercrimes did not involve monetary loss, while the other cybercrimes caused an average of one million dollars of damage. The primarily endangered interests are of private sector. The guardianship of the victims is surprisingly weak, vulnerable to the uncomplicated cybercrimes. The punishments (both imprisonment and fine) against cybercrime are generally light.

Keywords: Cybercrime, Criminality, Victimization, Profile of Cybercriminal

I Introduction

The social change of recent decades has been primarily symbolized by the development of information and communications technology. One of the most significant negative impacts in this context is the emergence and rampancy of cybercrime. The research on criminal phenomenon related to information and communications technology has become a focus of criminology, criminal law and information security.

Cybercrime is a comprehensive topic and attracts scholars from different disciplines to deal with. Many have been written about the theoretical explanation of cybercrime. Many findings about cybercrime in different studies revealed different dimension of multi-dimensional phenomenon. While the limited previous first-hand exploration have been widely accepted and cited, controversies and misleading exist among various studies. The

UOLTJ
About the Journal
Journal Articles
Submissions
Call for Papers
Citation Style
Copyright
Internship Course
Subscription Info
Contact Us
En français
UOLTJ Home

university of ottawa **law & technology** journal
revue de **droit & technologie** de l'université d'ottawa

Search Articles:
Search

Faculty of Law
Common Law Section

Law & Technology Program
University of Ottawa

open access law canada

science commons

Professor Elizabeth F. Judge

Editor and Faculty Advisor

The University of Ottawa Law and Technology Journal (UOLTJ) (ISSN 1710-6028; ISSN 1715-006X) is a bilingual (French and English), faculty-run, peer-reviewed academic journal devoted to scholarly articles on all aspects of law and technology. The Journal is interested in work on all aspects of this field, regardless of the type of technology, substantive area of law at issue, or theoretical or philosophical focus. The Journal is published in print and electronic formats.

In addition to printed issues, articles published in the Journal are also available in the electronic databases of Quicklaw, Westlaw, Lexis and Hein Online.

Call for papers

© University of Ottawa
If you are looking for additional information, please contact us.
Technical questions or comments about this site? webmaster@uoltj.ca
Last updated: Nov 17 2007

- Any questions?

Cybercriminology: Defence

Xingan Li, LLD
Faculty of Law
University of Turku

DOI: 10.13140/2.1.1538.8967

Hacker Subculture Defence

- What is a hacker? Two interpretations:
  - A talented and skilled programmer
  - A cybercriminal

Hacker Subculture Defence

- Steven Levy's 1984 book, Hackers: Heroes of the Computer Revolution. Levy came up with six tenets:

- Access to computers - and anything which might teach you omething about the way the world works - should be unlimited and total. Always yield to the Hands-On imperative!
- All information should be free.
- Mistrust authority - promote decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degress, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

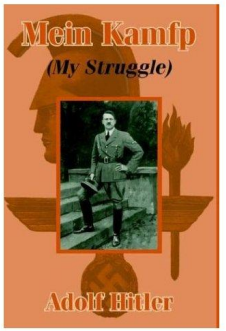
Hacker Subculture Defence

- Hackers do not usually consider unauthorized access as either harmful or damaging.

Trojan Horse Defence

- Example of Trojan Horse defence

Free Speech Defence



- In November of 1999, amazon.com caved in to legal pressure to cease selling English translations of *Mein Kampf* to customers in Germany. (Sales of the original German were already banned.) The Wiesenthal Center, which boasted about its role in this act of censorship, evidently believes that people can't be trusted to make up their own minds.

Free Speech Defence

- Many reasons have been given for not criminalizing the advocacy of any idea. These include:
- that open debate is necessary to the establishment of truth.
- that governments will inevitably abuse the power to prosecute ideas, inventing charges and twisting people's words in order to convict them.
- that people can't agree on which ideas should be criminalized. When the defining term is based on an emotion ("hate"), there is no limit on the subjectivity with which the laws can be applied.
- that driving a bad idea underground gives it an aura of martyrdom, and allows its advocates to claim that those who suppress it can't afford to let it be heard.

Source: Gary McGath, **In Defense of "Hate Speech", 2000, http://www.mv.com/ipusers/mcgath/hatespeech.html**

- Any questions?